SYSTEMS ENGINEERING RESEARCH CENTER

A US Department of Defense University Affiliated Research Center

SERC 2019-2023 Technical Plan

The Systems Engineering Research Center (SERC) is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology, Hoboken, NJ, USA.

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) under Contracts H98230-08-D-0171 and HQ0034-13-D-0004.

Table of Contents

Executive Summary ... iv

1 SERC Vision ... 1

2 Sponsor Needs ... 3

3 SERC Response To Sponsor Needs ... 5

4 Objectives, Principles, Approach and Transition Planning ... 14

4.1 Objectives ... 14
4.2 Approach ... 15
4.3 Transition Planning ... 15

5 Focus Areas, Programs, and Projects ... 19

5.1 Enterprises and Systems of Systems (ESOS) Research Area ... 20
5.1.1 ESOS Vision and Current Progress ... 20
5.1.2 Strategies to Address the ESOS Research Challenges ... 22
5.1.3 Comprehensive Enterprise / SoS Modeling and Analysis Program ... 23
5.1.4 Mission Engineering Program ... 28
5.1.5 ESOS Area Non-Core Funded Projects ... 30
5.2 Trusted Systems (TS) ... 30
5.2.1 TS Vision and Current Progress ... 30
5.2.2 Strategies to Address the Trusted System Vision ... 33
5.2.3 Systemic Security Program ... 35
5.2.4 Systemic Assurance Program ... 41
5.2.5 TS Area Non-Core Funded Projects ... 50
5.3 Systems Engineering and Systems Management Transformation (SEMT) ... 51
5.3.1 SEMT Vision and Current Progress ... 51
5.3.2 Strategies to Address the SEMT Vision ... 53
5.3.3 Digital Engineering Program ... 54
5.3.4 SE Methods for AI and Autonomous Systems Program ... 65
5.3.5 Systems Engineering for Velocity and Agility Program ... 68
5.3.7 SEMT Area Non-Core Funded Projects ... 72
5.4 Human Capital Development (HCD) ... 73
5.4.1 HCD Vision and Current Progress ... 74
5.4.2 Strategies to Address the HCD Vision ... 76
5.4.3 Evolving Body of Knowledge Program ... 77
5.4.4 Experience Acceleration Program ... 80
5.4.5 Systems Engineering and Technical Leadership Education Program ... 82
5.4.6 Emerging/Critical HCD Areas Program ... 85
5.4.7 HCD Area Non-Core Funded Projects ... 85
5.5 Infrastructure Development ... 86
5.5.1 SERC Website ... 86
5.5.2 SERC Innovation and Demonstration Lab (SIDL) ... 86

6 New Project Initiation ... 88

Acronyms and Abbreviations ... 89

EXECUTIVE SUMMARY

This Systems Engineering Research Center (SERC) 2019-2023 Technical Plan aligns the SERC Vision and Research Strategy with the Sponsor's Core funding priorities. It describes the SERC Vision, the Sponsor's needs, and the SERC's response to these needs. This is reflected by 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). A Vision statement is presented for each of these four Research Areas, along with a strategy to address it. Eleven research programs have been identified to support this strategy. Research projects are then presented which support each of these programs, consisting of existing and anticipated future projects.

This 2019 – 2023 Plan follows the initial 2014 – 2018 Technical Plan that was approved by the Assistant Secretary of Defense for Research and Engineering in October 2013 with annual Core funding appropriated for its support. More than sixty projects have been executed since the original Technical Plan was published, some to completion, others still ongoing. These projects have been delivering methods, processes, and tools (MPTs) in each of the four Research Areas that define the SERC research portfolio. Transition has also been ongoing and growing, with many acquisition programs and defense organizations piloting and adopting SERC MPTs as those MPTs have matured. Since October 2013, when the SERC began executing this plan, SERC researchers have delivered more than 300 papers and technical reports, and prototype software implementations of their methods and processes. Equally important, SERC collaboration and infrastructure have grown significantly.

It has been noted that the original plan was successful in creating synergy between projects and programs within research thrust areas, serving as a framework for resource allocation, supporting evolving programs to satisfy changing needs and increasing the rate of adoption and impact. However, the plan had shortcomings in providing synergy between research areas, supporting engineering of mission-wide capabilities with demonstrable returns, and broad adoption and impact at a rapid pace into the educational system.

In this new plan, three mission areas have been added to reflect the growing importance of several specific areas of challenge and also to provide synergy between the four Research Areas. The Grand Challenges for each Research Area have been replaced with Visions to more accurately reflect their aspirational nature. In addition, increased emphasis has been made on the transition of research results into education.

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

The Visions in each Research Area that support these Missions are:

ESOS - *Create the foundational SE principles and develop the appropriate MPTs to enable the DoD and its partners to model (architect, design, analyze), acquire, evolve (operate, maintain, monitor) and verify complex enterprises and systems of systems to perform mission engineering in a manner that generates an affordable and overwhelming competitive advantage over its current and future adversaries.*

TS - *Achieve much higher levels of mission trust by applying the systems approach to achieving system assurance and trust for the increasingly complex, dynamic, autonomous, cyber-physical-human net-centric systems and systems of systems.*

SEMT - *Develop methods, processes and tools to enable the transformation from sequential, document-driven, hardware-centric, highly constrained practices toward much faster OODA-loop-supporting mission and enterprise-oriented, cyber-physical-human, value-focused, model-driven, full life cycle system creation and delivery processes.*

HCD - *Discover how to dramatically accelerate the professional development of highly capable systems engineers and technical leaders in DoD and the defense industrial base to address the challenges created by the rapidly changing nature of systems, and systems of systems, and the human capabilities necessary to support them, and determine how to sustainably implement those discoveries.*

The SERC, guided by this Technical Plan, will deliver the greatest impact for DoD and the Intelligence Community (IC) by:

1. *Conducting* long-term research that makes significant progress on the Missions and Research Area Visions
2. *Transitioning* that research into practice within DoD, the IC, defense industrial base, and other federal agencies; and by developing more powerful ways to facilitate such transition
3. *Amplifying* sponsor resources by forging relationships with other organizations that become partners, contributing their resources and energy to the SERC and adopting SERC research
4. *Strengthening* the existing SERC culture, mechanisms and focus on collaboration
5. *Instituting* new approaches to educate future systems engineers and engineers that leverage the full strength and diversity of the collaboration

The strategy described in this Technical Plan embraces these operating principles. As was done in original Technical Plan, after receiving an initial core funding level for two years funding for each individual Research Topic (RT) will be reduced by approximately 20% per annum through the end of 2023. This reduction incentivizes Principal Investigators (PIs) to seek complementary funding from non-Core sources. Core funds freed up through this strategy accumulate in an investment pool that funds new programs and projects. Besides $25M previously spent on projects that became Core funded in 2014 through 2018, the SERC was awarded more than $38M in 2014-2018 on projects that completed. Projects that completed prior to 2019 are not addressed in this plan.

1 SERC VISION

In the original Technical Plan published in 2013, the vision for the SERC at the end *of 20*18 was stated as:

- IMPACT: The SERC has indeed become the go-to place for high-quality SE research and exploratory development. Its research is widely applied in DoD and the defense industrial base with tangible impact affecting billions of dollars of acquisitions; its research results are woven into the curricula of dozens of university programs (including many outside the set of SERC Collaborators) that are educating thousands of students.
- RECOGNITION: The SERC includes ten of the US News and World Report (USNWR) top-25 Industrial/Manufacturing/Systems Engineering departments.
- STUDENTS: SERC Collaborators graduate over half of the US MS-SE and PhD-SE graduates per year. Many PhD graduates join other SERC universities as faculty or staff, significantly increasing the breadth and depth of research collaborations. Collaborators attract and educate the best students, drawn from current DoD and defense industrial base employees and from those who are attracted to systems engineering by the vigor and quality of Collaborator educational programs.
- LEADERSHIP: The SERC provides much of the leadership in SE-related professional societies, increasing collaboration among them. It continues to operate and grow the Conference on Systems Engineering Research as the premier SE research conference, along with feeding its papers into the leading SE-related journals.
- KNOWLEDGE: The SERC operates the world's largest and most-visited SE research website, including the largest and best-organized SE research experience base. It continues to provide leadership in evolving the SE Body of Knowledge. It runs the most widely attended and highest-rated SE webcast series.
- SCALE: The SERC has become a $20M/year enterprise: $5M of Core funding from ASD(R&E); $5M from other sponsors in the DoD/IC; $5M to apply research results in pilots with DoD operational organizations; and $5M in research and pilots from outside of DoD. Thus, each $1 of Core funding attracts an additional $3 of outside funding.

Over the past five years, progress towards that vision includes:

- IMPACT: Although its footprint is still small, SERC research is being used in all Services, in the defense industrial base, and in academia – and that research use is steadily growing. For example, the Marines are using SERC-developed tools for tradespace analysis and systems portfolio analysis; the Navy is adopting SERC model-based systems engineering techniques; the Air Force is applying SERC cost modeling approaches to manage complex systems; both the Army and Defense Acquisition University are applying SERC approaches to growing technical leaders; several defense contractors are applying research on how to improve the effectiveness of their systems engineers; and many universities have adopted SERC developed approaches to weave systems thinking and systems engineering into engineering capstone projects. The adoption of SERC technology is expected to grow significantly over the next five years, primarily as a result of the SERC's greater focus on transition and because the SERC has an ever-expanding portfolio of maturing research available to early adopters.

- RECOGNITION: The SERC Collaborator membership is proving to be more stable than anticipated when the Technical Plan was originally written in 2013. Six SERC Collaborators are in the top 25 in the 2018 USNWR rankings for Industrial/Manufacturing/Systems Engineering programs.
- STUDENTS: During this coming year, the SERC will collect data to measure progress against this aspect of its vision.
- LEADERSHIP: Faculty members from SERC Collaborator universities have played key roles within the International Council on Systems Engineering (INCOSE), the Accreditation Board for Engineering and Technology (ABET), the American Institute of Aeronautics and Astronautics (AIAA), and other professional societies; e.g., a Massachusetts Institute of Technology professor was the Editor-in-Chief of the Systems Engineering Journal and a Georgia Tech professor is the Editor-in-Chief of the Journal of Enterprise Transformation.
- KNOWLEDGE: This year the SERC has launched a new website which provides a much-improved platform to host and disseminate important knowledge about systems engineering and about SERC research. Starting in 2016 the SERC began offering webcasts on its research and related topics. The SERC is one of the three organizations sponsoring the Systems Engineering Body of Knowledge, which has become one of the most prominent online source of information about systems engineering – http://www.sebokwiki.org/ averaging approximately 20,000 visitors monthly.
- SCALE: During government FY 2018, SERC awards totaled approximately $10M, including $5M in Core funding. Growing total awards to $20M will be challenging but is feasible.

2 Sponsor Needs

The outlook on SE needs for 2019-2023 reflects a sense of urgency on the part of the Department of Defense to maintain technical advantage over military adversaries. SE is seen as an enabler for safe, secure, and rapid introduction of new technology, but it must adapt to new levels of complexity and pace of response. The Office of the Undersecretary of Defense for Research and Engineering OUSD(R&E) has identified three efforts to pursue sustained technological advantage: mitigating current and anticipated threat capabilities, affordably enabling new capabilities in existing military systems, and creating technology surprise through science and engineering. As part of these efforts, OUSD(R&E) identified the following priorities for DoD engineering shown in Figure 2-1 below.[1] These span the SERC's research areas and the associated priorities strongly reflect the three mission areas.

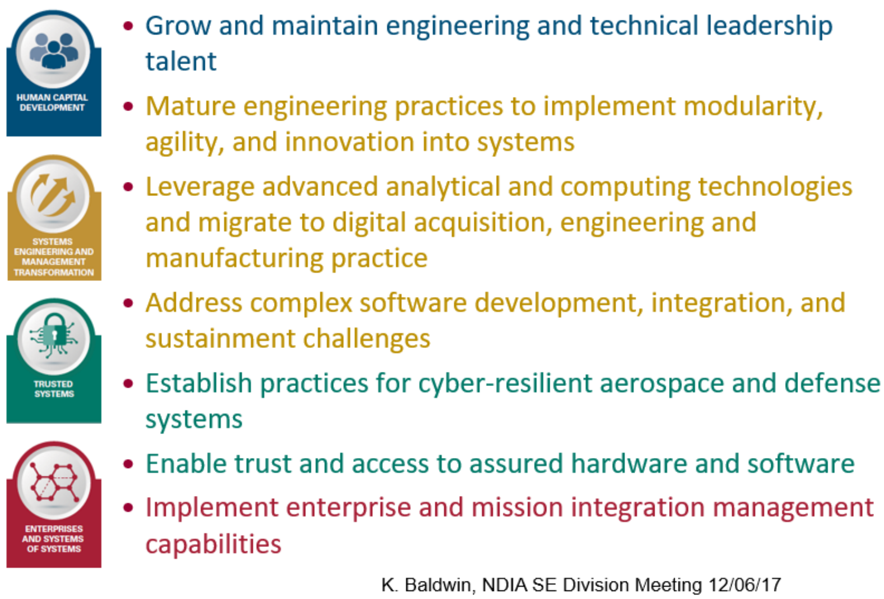

Figure 2-1: OUSD(R&E) Priorities for DoD Engineering

The DoD is working to rapidly mature sets of emerging technologies, to include:[2]

- Leveraging autonomy and artificial intelligence to operate inside an adversary's decision cycle
- Greatly expanding manned-unmanned combat teaming to extend our attack surface
- Re-amplifying our guided-munitions advantage with 'raid-breaking' capabilities
- Creating new mass by disaggregating complex systems to deliver combined effects
- Developing 'inside-out' and 'over-under' capabilities that leverage dispersal, sanctuaries, and speed
- Developing new forms of distributed maneuver that combine kinetic, EW, and cyber effects

---

[1] K. Baldwin, National Defense Industry Association Systems Engineering Division meeting, December 6, 2017.

[2] M. Miller, 18th Annual National Defense Industries Association Science and Emerging Technologies Conference, April 18, 2017

These strategies challenge the traditional roles and methods of SE. We refer to autonomy and artificial intelligence, as well as manned-unmanned teaming, as the “AI and Autonomy” mission area because the ability of these systems to learn and adapt defies traditional SE processes that focus on control and validation of requirements. There is a need to “rethink” many traditional SE methods, processes, and tools to support the development and test of these systems. Operating inside the adversary’s decision cycle; Observe, Orient, Decide, Act; or ‘OODA’ loop,[3] is in fact a systems approach to mission execution. However, OODA in the science and technology (S&T) process implies a much leaner and more agile approach to the development and deployment of system capabilities. This is our “velocity” mission – how to maintain rigorous SE discipline while greatly increasing the speed and adaptability of products and capabilities. In this process, the SE discipline must also move toward having the capability to support more compositional system development and sustainment strategies. Large scale development of highly complex systems for single mission purposes must be replaced by systems that can be rapidly composed from new and existing capabilities and deployed in a ‘build-measure-learn’ cycle of prototyping, experimentation, and incremental delivery. Finally, all of these strategies must be met while assuring the safety and security of these systems in the presence of a cyber-enabled adversary. This is the security mission – ensuring our future system capabilities are resilient to adversary attacks at all levels from mission to components.

[3] OODA- Observe, Orient, Decide, Act

3 SERC Response To Sponsor Needs

The SERC is a large network of universities with access to the best science, engineering, and technology related faculty, students, and research in the nation. To respond to DoD needs, we need to provide access to all faculty in all disciplines who have interest in systems-oriented research. The challenges our sponsor faces are multi-disciplinary and need a collaborative response from the best of the best across the SERC university network. The SERC research portfolio has always been multi-university and multi-discipline, and SERC leadership must continue to nurture and grow those collaborations. In this way the SERC can serve as a networker to the SE community addressing core and emerging DoD challenges.

SERC workshops convene communities across government, academia, and industry to discuss emerging and future SE needs and develop the research agendas that address our sponsor's engineering challenges. In the last two years, six workshops set the stage for research across the sponsor listed priorities:

- The **Model Centric Engineering Forum** addressed the transformation toward digital and model-based engineering
- **Modular Open Systems Approach (MOSA): Towards Cost Effective Acquisition Strategy** convened a discussion on the modular and open systems ecosystem and positive impacts of modularity
- A workshop on **Cyber Social Learning Systems** looked at future SE needs for rigorous and safe engineering of human intensive, AI-enabled cyber-physical systems
- The **Systems Ontology Bootcamp** introduced attendees to the concepts of digital ontologies and addressed the development of robust system ontologies for future digital engineering
- A workshop on **Model Based System Assurance** convened approximately 60 system and software engineers to discuss next-generation system assurance design and test via digital engineering
- The **Managing Program Acquisition and Program Risk** workshop explored where research might bring methods, processes, and tools to improve program risk management.

The SERC will continue to work with the sponsor to identify critical areas of interest and conduct at least three workshops per year to engage the SE community across the DoD's core challenges.

In addition, the "SERC Talks" series of bi-monthly research webinars brings leading researchers from the SE community to share their insights on critical SE challenges. Topic areas to date include ten talks covering Model-Centric Systems Engineering, Cyber-Physical Learning Systems, and Cybersecurity. The series will continue to cover emerging research across the sponsor priority areas. Finally, the development of the SERC NAV, short for Network Analysis and Visualization Tool, was developed to link professors, universities, research projects, publications, and metadata across the SERC ecosystem.

These convening activities set the stage for and provide the founding ideas and needs for future SERC research. In the 2019-2023 Technical Plan, we are adopting the OODA concept as a central driving strategy for our research portfolio. The community events serve as the "Observe" stage of the loop, where regular workshops and community engagements attract a much broader set of perspectives than any one SERC partner can gain, with the goal to continually update and redefine SERC research strategies.

In the "Orientation" phase, the SERC research network will take a broad leadership role in the development of the future roles and disciplines of SE, bringing the practice into a digital age that gradually replaces the traditional static artifacts of the SE process with dynamic, collaborative, and interactive methods and tools for more agile and informed decision making. Where previous Technical Plans focused on improving the state of the art in SE, this and future plans will focus on leading the community to address the world's grand challenges. This will start with the three challenges and mission areas introduced in this plan.

In the "Decide" phase of the OODA loop, there is a hierarchy of decision processes where SERC researchers and their institutions can engage. At the highest level, SERC research will embrace and lead the future evolution of SE practice and discipline, addressing a world where complexity, speed, and automation will radically change the nature of engineered systems. In the middle tiers, SERC researchers will engage with our sponsors to inform and develop system roadmaps and strategies, leveraging the full resources of our partner universities. At the lowest level, SERC researchers will rethink and develop SE methods, processes and tools that radically improve decision making in response to the complexity of future system challenges. SERC research will address the significant gaps and challenges for both the SE community and the engineering and program management communities that employ SE disciplines.

In the "Act" phase, the SERC will partner with our sponsors and users to prototype, experiment, and test the latest SE innovations as well as develop the methods, processes, and tools for a more agile and adaptive SE community.

The SERC actively manages its research portfolio, looking for and nurturing synergies between projects, programs and research areas. The SERC works with its sponsor to identify projects that can have greater impact on DoD's strategic SE research needs. One such approach is the New Project Incubator, described in Section 6, in which SERC Collaborators propose new research ideas, with the most promising projects being given limited funds to support their early development.

Long-term project funding has been especially evident since 2012, when the majority of new funding began being spent on multi-year higher-impact projects. Most projects are now being conceived and proposed as multi-phase, multi-year efforts that are synergistic with other projects in their program and research area; for example, the *Experience Accelerator* Project, which is attempting to develop ways to greatly reduce the time needed to mature an effective systems engineer, is being executed as a 5-year project to deliver a strong foundational capability, validate it, and transition it to early adopters and is synergistic with the Helix Program within the Human Capital Development research area. In this technical plan, the synergistic efforts have been expanded to the mission level, tying together research from all four Research Areas as shown below. Additional sponsors and funding are being sought to continue growing that capability and to deliver even greater value, consistent with the *SCALE* element of the SERC vision described earlier in Section 1.

The DoD's critical systems challenges can be summarized in the following three missions (as shown in Figure 3-1):

> **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)
>
> **Security:** Designing and sustaining the demonstrable ability to safeguard critical technologies and mission capabilities in the face of dynamic (cyber) adversaries
>
> **AI & Autonomy**: Developing and supporting system engineering MPTs to understand, exploit and accelerate the use of AI and autonomy in critical capabilities

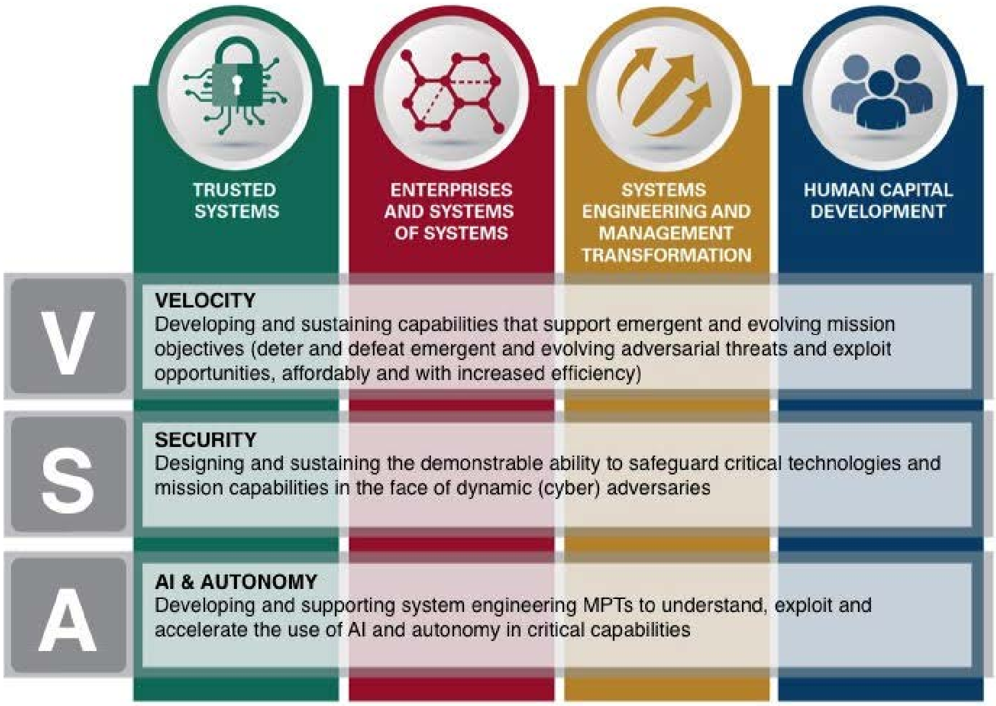

Figure 3-1: The Three Major Missions which Provide Synergy to the Thematic Areas

Each of these missions provides a synergistic touch point for each of the research activities in the four research thematic areas that were developed in the first SERC Technical Plan and are expanded in this plan as shown in Figure 3-2 and described below.

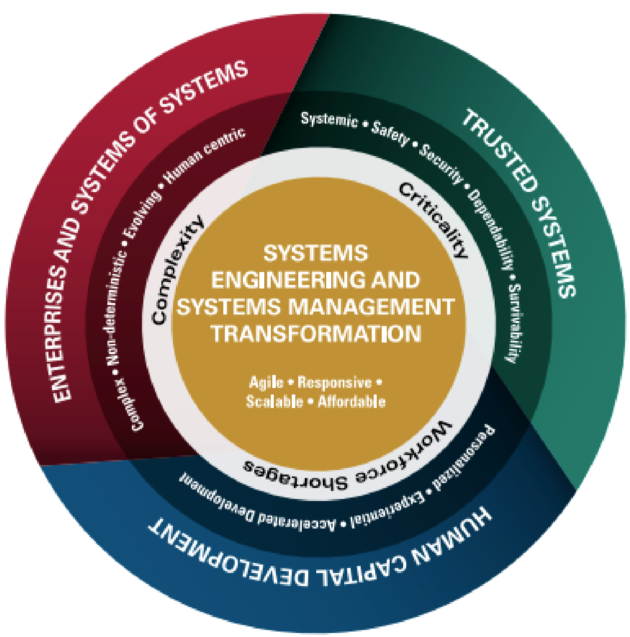

Figure 3-2. The Four Thematic Areas Being Addressed by SERC Research Tasks and Priorities

Enterprises and Systems of Systems: Mission Engineering (ME) has become a core focus area for the DoD. ME treats the end-to-end mission as the system of interest in defense programs. Today systems engineering must be applied to the systems of systems (SoS) supporting operational mission outcomes. Complexity drives the adoption of enterprise processes that help manage the complexity and resultant cost of today's systems. Section 855 of the fiscal year 2017 National Defense Authorization Act (NDAA) states a need for "sponsoring and overseeing research on and development of (including tests and demonstrations) automated tools for composing systems of systems on demand." There are limited methods, tools and data that support the proper integrated analysis bridging engineering and mission analysis across the lifecycle. These methods are needed to help understand interdependencies across Systems of Systems (SoS) and emergent effects. In addition, the mission level view drives two other significant sponsor priorities: effective use of modular and open systems approaches, and digital engineering transformation:

- The National Defense Authorization Act (NDAA) tasks acquisition programs to employ a Modular Open Systems Approach (MOSA) which emphasizes an enterprise process for program and portfolio management. Although the services have emphasized and assessed programmatic response to MOSA imperatives for a number of years, these assessments have been qualitative and have had little impact on either the culture of the DoD program ecosystem or on the requirements baselines for development and sustainment. Near-term SERC research should focus on methods, processes, and tools that codify knowledge of successful MOSA strategies, quantify associated MOSA architecture attributes and incorporate them into early stage acquisition tradespaces, and instill an adaptive requirements culture in the acquisition workforce.

- Digital Engineering (DE) and related model-based engineering methods will be core to the development of meta-models and meta-functions that link systems and missions. Although the SERC has been at the forefront of DE pilot programs, the enterprise challenge will be to shift over time the primarily paper-driven development and acquisition processes to digital artifact use. Research is needed to create the enterprise infrastructures needed, innovate and enable new practices, and realize the speed and efficiency of digitalization and eventually automation. The linking of mission engineering skills in a data-driven enterprise will ultimately drive the need for a more technologically-based acquisition workforce, and the DoD must continue to grow their engineering and technical leadership talent.

With respect to ***Velocity***, there are three enterprise challenges needing near-term research: leading an agile enterprise transformation at scale, creating a culture of continuous development and delivery of military capabilities, and building the digital engineering factory as an infrastructure for development, test, and deployment operations. The leadership challenge is significant: how do you design an agile leadership framework and agile systems development when the DoD "enterprise" is fragmented across industry and government agencies? The means to optimize information flows and associated processes is a critical research area. The continuous development and delivery problem is dependent on this framework but also on how user feedback mechanisms are designed directly into systems. New patterns that consider direct user feedback as system requirements and design strategies will be necessary and have not often been considered in SE processes. The factory model is a solution space for this framework, and from an enterprise view there is a need for the SERC to collect, develop and exchange best practices across both government and industry.

For ***Security***, ESOS research is needed to address the human aspects of cyber risks, particularly in the engineering enterprises that develop and deploy defense and other government systems. As AI and related machine learning algorithms become more predominant in the cybersecurity domains, there is a need to address human-machine teaming aspects of cyber operations. This needs to be extended into the mission operation domains, where knowing when systems are compromised is critical. An emerging research area is the use of machine learning in the automation of parts of situational awareness functions, which can apply in many domains.

AI and Autonomy: At the core of the challenges of artificial intelligence and increasing automation is the need for better methods and tools to understand, predict, and validate the emergence properties of future systems that learn. Without a strong linkage to mission and enterprise concerns, requirements for these future systems will be impossible to define and verify. The resulting Human-Machine interaction is fundamentally a SoS problem. The DoD has listed core systems engineering research needs for methods and tools that properly define human-machine function allocation; and development of tools and techniques that enhance trust, apply formal methods to assure autonomous system behaviors, and enable rapid development and certification.

Trusted Systems: Today's weapon systems are highly connected, and the resulting connectivity and complexity leads to vulnerabilities in the systems that are often not known until they are operational. The need for improved assurance of these systems begins with mission assurance and drives new methods, processes and tools that can assure better safety and security at design time. Traditional hierarchical analysis of safety and security is failing as complexity grows and external connectivity increases. The DoD Cyber Resilient Weapon Systems initiative recognizes that with the cybersecurity threat, individual systems and components cannot be individually assured. Analysis of mission level resilience is a core systems engineering need. Research that supports "designing in" security is needed. This research area is at the core of the ***Security*** mission area.

Velocity is a challenge for weapon systems in the domain of cyber resilience. For systems at the forward edge of the mission, it is unlikely that weekly software patches to correct security vulnerabilities will ever be the norm; the means to rapidly update, reconfigure or adapt the system in response to emerging cyber threats is a necessity. Automation of design checking in early program decision stages is also a critical near-term research need, as today's systems-of-systems are already beyond the scale of manual attack tree and hazard analysis methods.

Increasing automation and resulting dynamic models of trust and assurance pose key challenges for future systems. In the ***AI and Autonomy*** mission area there is a need to understand the consequences of self-learning systems as both a major competitive advantage to the DoD, as well as an assurance, evaluation, and certification concern. The systemic nature of these concerns also creates a need for an increasingly technical systems engineering workforce.

System Engineering and System Management Transformation: The battlefield of the future will be dominated by adaptive capabilities and technology. Toward this end, weapons systems are becoming more flexible, more modular, and more autonomous. The DoD will depend on the transformation of systems engineering to develop and manage these systems, and to speed the delivery of new capabilities and new technology to the warfighter, helping the warfighter adopt new methods of fighting to take advantage of the new capabilities.

Toward this end, the transformation of systems engineering will focus on:

- Using digital engineering to rewire the system development process, provide guidance to design engineers in the form of models rather than natural language specifications, and propagate changes instantaneously across large dispersed development teams;
- Developing a new approach to designing autonomous systems, particularly in the areas of requirements, verification and validation, so that reliable systems can be developed with novel and adaptive behaviors;
- Developing a rigorous strategy for effective and rapid Mission Engineering and supporting the strategy with MPTs for mission design and mission decision-making.

The implications of Digital Engineering to this thematic area will be significant with respect to ***Velocity***. As the full engineering development, test, manufacturing, and support lifecycles become digitally interconnected, there is tremendous potential for increased speed and efficiency via digital information exchange. This is an area where there is tremendous innovation opportunity. Research incubator projects and perhaps innovation challenge competitions that exploit piloted digital threads and digital twins can be a focus.

In the ***Security*** mission area, the traditional decomposition and analysis methods are insufficient to support designs that counter the cybersecurity threat. There is ongoing research in this area, much of it in the Trusted Systems thematic area. Research projects that aim to institutionalize cyber resilient design practices across the SE discipline are needed. An initial research area is in the development of effective risk/cost models for both lifecycle cost and program effort. Another immediate research need is associated with effective risk-driven requirements that reduce risk to the lowest level given cost, schedule and performance constraints.

In the ***AI and Autonomy*** mission area, there will be many challenges. For example, the link between what the machine learns and its functional requirements is almost accidental at this stage of technology development, and formality is needed in the process. Human Systems Integration (HSI) moves to the forefront of the system design process in the manned-machine teaming context, but HSI practices are still poorly integrated into SE. Research associated with new types of simulation environments that allow human and machine interactions to emerge in a representative and measurable environment is greatly needed.

Human Capital Development: Providing ways to ensure that the quality and quantity of systems engineers and technical leaders enables a competitive advantage for the DoD and defense industrial base. All of the sponsor’s systems engineering challenges reflect the need for a more technical workforce that can adapt to rapidly emerging technological trends. Cross-disciplinary and cross-program knowledge and collaboration are a necessity. Due to their interconnected nature, systems today and in the future increasingly stress the capabilities of a single person to fully grasp their operational dimensions. Attributes like complexity, composability, agility, and resilience imply a dramatically increased need to develop systems thinking and systems architecture competencies in the future workforce, as well as leadership and change management abilities. In addition, there are the growing challenges of generational change in the workforce that must be met to ensure that the knowledge of not only the “how”, but the “why” in our current systems is captured and used by our future workforce.

To improve ***Velocity***, all systems engineers and related leadership, program management, and acquisition roles need to become adept at managing systems in rapidly changing environments. This means consideration and adoption of continuous development and deployment strategies need to become a culture and need to pervade every level of the defense systems enterprise. There is a need to match rapidly evolving commercial practices to the characteristics of defense systems, and then to educate and train the workforce to move to this type of culture.

System ***Security*** engineering has a new context in DoD weapon systems introduced by information connectivity and potential cyber adversaries. Human capital development in this field is seriously under-developed. Research needs include better taxonomies, a competency model, better understanding of roles in different lifecycle phases, and curriculum guidance. Also needed are professional development courses, and an assessment of certification requirements and opportunities.

In the ***AI and Autonomy*** mission area, one specific area of focus is the test and certification of autonomous systems. There are new paradigms forming in this area and the requisite knowledge, skills, and abilities are lacking. Too much work is focused on developing competencies for creating and using autonomy, little is focused on the test and evaluation side.

Vision Statements: Each of the Research Areas are supported by the following Vision statements (referred to as "Grand Challenges" in the previous SERC Technical Plan) that provide inspirational direction to their work.

- **Enterprises and Systems of Systems:** *Create the foundational SE principles and develop the appropriate MPTs to enable the DoD and its partners to model (architect, design, analyze), acquire, evolve (operate, maintain, monitor) and verify complex enterprises and systems of systems to perform mission engineering in a manner that generates an affordable and overwhelming competitive advantage over its current and future adversaries.*
- **Trusted Systems:** *Achieve much higher levels of mission trust by applying the systems approach to achieving system assurance and trust for the increasingly complex, dynamic, autonomous, cyber-physical-human net-centric systems and systems of systems.*

  System Engineering and System Management Transformation: *Develop methods, processes and tools to enable the transformation from sequential, document-driven, highly constrained practices toward much faster, flexible OODA-loop-supporting mission and enterprise-oriented approaches enabled by advances in modeling, simulation, data-driven analysis and artificial intelligence.*
-
- **Human Capital Development:** *Discover how to dramatically accelerate the professional development of highly capable systems engineers and technical leaders in DoD and the defense industrial base to address the challenges created by the rapidly changing nature of systems, and systems of systems, and the human capabilities necessary to support them, and determine how to sustainably implement those discoveries.*

These four thematic areas are further divided into the eleven programs described below. These programs have the potential to make a transformative impact on DoD and the IC. The SERC Research Council[4], which includes some of the most capable researchers in the field, continues to help shape this portfolio.

[4] See http://www.sercuarc.org/serc-research-council/.

- **Enterprises and Systems of Systems**
    - *Comprehensive Enterprise / SoS Modeling and Analysis:* Create, validate, and transition Methods, processes, tools (MPTs), and insights required to shape our enterprises, architect our SoS capabilities, and engineer our missions with sufficient "velocity" so that their capabilities remain effective in rapidly changing environments
    - *Mission Engineering (New):* Identify and prototype the methods, processes and tools to rapidly compose missions utilizing flexible and modular systems in conventional battlefields and special operations, space, and cyberwarfare.
- **Trusted Systems**
    - *Systemic Security:* Create, validate, and transition MPTs to ensure systemic security using knowledge of system objectives and operation
    - *Systemic Assurance:* Create, validate, and transition MPTs to provide systemic assurance of safety, reliability, availability, maintainability, evolvability, and adaptability.
- **Systems Engineering and Systems Management Transformation**
    - *Digital Engineering (formerly Interactive Model-Centric Systems Engineering):* Develop tools and methods that fill in the seams in the digital engineering toolsets which are becoming the backbone of DoD development of complex systems.
    - *SE Methods for AI and Autonomous Systems (New):* Develop and prototype MPTs for requirements generation, verification testing, and validation testing for learning, intelligent, autonomous systems, where system behavior cannot be conventionally specified during development.
    - *Systems Engineering for Velocity and Agility (formerly: Affordability and Value in Systems, Quantitative Risk, & Agile Systems Engineering):* Utilize systems engineering to dramatically accelerate weapon system development by balancing speed, performance, cost and risk in every design and development decision, from pre-Milestone A to Initial Operating Capability.
- **Human Capital Development**
    - *Evolving Body of Knowledge:* Establish active communities and mechanisms that create and support living bodies of SE knowledge
    - *Experience Acceleration:* Develop an open source community that creates, validates, and transitions technology and content for the use of experiential technology to educate systems engineers and technical leaders
    - *SE and Technical Leadership Education:* Create, validate, and transition curricula and practices to support the instruction and learning of systems and technical leadership for inexperienced students in college and experienced professionals
    - *Emerging/Critical HCD Areas:* Track the changes in emerging/critical SE workforce needs, demographics and performance over time determine necessary advances to satisfy future HCD needs.

Research Program Progress to Date

Between October 1, 2013 and June 1, 2018 research on the eleven programs in the Technical Plan has been packaged into more than 100 projects which have been awarded more than $26M in Core funds plus more than $12M from other DoD organizations, including all the Services, Defense Acquisition University, and elements of the Intelligence Community. In several cases, those non-Core funds augmented existing projects. These projects have been delivering methods, processes, and tools (MPTs) in each of the four Research Areas that define the SERC research portfolio, contributing towards achieving the research Visions. Transition has also been ongoing and growing, with many acquisition programs and defense organizations piloting and adopting SERC MPTs as they have matured. Since October 2013, when the SERC began executing the 2013-2018 Technical Plan, SERC researchers have delivered more than 300 papers and technical reports, and prototype software implementations of their methods and processes. All of these projects contribute towards achieving the Missions and Research Area Visions described earlier in the *Executive Summary.*

4 OBJECTIVES, PRINCIPLES, APPROACH AND TRANSITION PLANNING

4.1 OBJECTIVES

The SERC will have the greatest impact on the DoD and the IC by:

1. *Conducting* long-term research that makes significant progress on the Missions and Research Area Visions
2. *Transitioning* that research into practice within DoD, the IC, defense industrial base, and other federal agencies; and developing more powerful ways to facilitate such transition to be executed by external organizations
3. *Amplifying* sponsor resources by convening a broad SE community and forging relationships with other organizations that become partners, contributing their resources and energy to the SERC and adopting SERC research
4. *Strengthening* the existing SERC culture, mechanisms and focus on collaboration and multi-disciplinary problem-solving, engaging the full science, engineering, and technology faculty across the SERC partner universities
5. *Instituting* new approaches to educate future systems engineers and bring systems approaches across the breadth of engineering disciplines that leverage the full strength and diversity of the collaboration

These approaches align with the SERC's four Operational Principles:

1. Conduct innovative, high-impact research
   a. Focus on research efforts that have the potential of increasing the security and prosperity of the nation
   b. Focus on research which addresses future systems needs
   c. Focus research efforts on systems which can be generalized beyond a given domain and transform the discipline
   d. Only perform tasks which are research oriented (usually publishable when not classified or otherwise restricted)

2. Translate proof-of-principle prototypes to impactful applications
   a. Work to ensure that there is a path from research results to impact for the security and prosperity of the nation

3. Strengthen and leverage the research network
   a. Convene groups across industry, academia, and industry that engage and set the priorities for future SE research
   b. Ensure that the research is conducted by the best available resources
   c. Bring in new Collaborators and partnering organizations and institutions who provide long-term strategic benefit
   d. Focus on creating a network of academics, industry and government that is sustainable

4. Prepare the next generation

   Provide a focus on education and training research, both in research on education and training, and in the actual education and training of researchers, graduate students, and practitioners

4.2 Approach

This technical plan expands upon the general approach used for the original 2013 – 2018 SERC Technical Plan areas. Much as the DoD is shifting focus from broad capabilities to more specific missions, so too the SERC is ensuring that the research in each thematic area contributes to these mission objectives. This is a natural evolution as the lines between the research thematic areas increasingly become blurred. The Grand Challenges that were created in the original Technical Plan have been updated to continue to provide supporting visions for each of the Research Areas as shown in Figure 3-2. These Visions were formulated to provide a point of integration between existing programs in each research thematic area, and also to provide opportunities to generate new, related research areas. The Missions and Research Visions also provide inspiration and an integration point for non-SERC universities, federally funded research and development centers (FFRDCs), other University Affiliated Research Centers (UARCs), DoD laboratories and industry researchers to perform collaborative research and provide natural transition into use. SERC management worked closely with the SERC Research Council[5], principal investigators and others to craft the Mission, Visions objectives, and strategy for each of the four Research Areas, and to lay out program descriptions, timelines, anticipated results, and resources required.

Additionally, this Technical Plan continues to assume that:

1. Researchers will be incentivized to find some of their resources outside of Core funds. This could come in the form of matching funds or other forms of resources.
2. Researchers will be incentivized to transition their results into practice. Each project will have a transition plan in place when the project begins with the opportunity for additional downstream funding to facilitate transition to practice and to develop educational materials and courses based on research results that will be shared by all SERC collaborating institutions.
3. Seed funding will be available to explore novel and promising ideas that may be the sources of future breakthroughs. Through an incubation grant open solicitation process with all of the SERC Collaborators, these ideas will be selected by the sponsors, SERC Research Council and SERC leadership. Two such solicitations have been successfully completed and will continue be made on a biennial basis.
4. Shared IT infrastructure will be available for use by every research project.

4.3 Transition Planning

Research in systems engineering is atypical. Traditionally, research discovers new ideas, new properties, or new relationships, leaving it to engineers to take these ideas and make them useful. Systems engineering research usually involves both the early discovery and their packaging for useful application. The value of systems engineering research is in ensuring that other systems engineers can more effectively

[5] See http://www.sercuarc.org/serc-research-council.

create value for their stakeholders. No matter what insights SERC researchers achieve through their research, they must be validated by practicing engineers and shown to be useful in effective development and evolution of safe, reliable, and useful systems. It is for this reason that the SERC includes transition as an increasingly important part of its research methodology and focus.

The SERC approaches transition in a number of ways, beginning when the research effort is first defined. Research plans specify a variety of transition actions. The goal is to get "useful combinations" of SE MPTs into the hands of SERC sponsors and stakeholders as quickly and efficiently as possible. MPTs are the SERC's technological output. Effective transition into application is key to providing real systems engineering research value.

As shown in Figure 4-1, many different customer motivations affect their readiness to adopt new technology. The initial target for SERC MPTs is the innovators and early adopters. A SERC MPT successfully transitioned to *innovators* and *early adopters* would be:

- Applied by a small number of practitioners, generally with substantial assistance from the research team
- Demonstrably and credibly delivering its intended value to *early adopters*
- Taught in university programs associated with the research team
- Published in several articles and conferences
- Sustained largely by SERC resources and infrastructure with some support from elsewhere that has the potential to scale up the ability for adoption

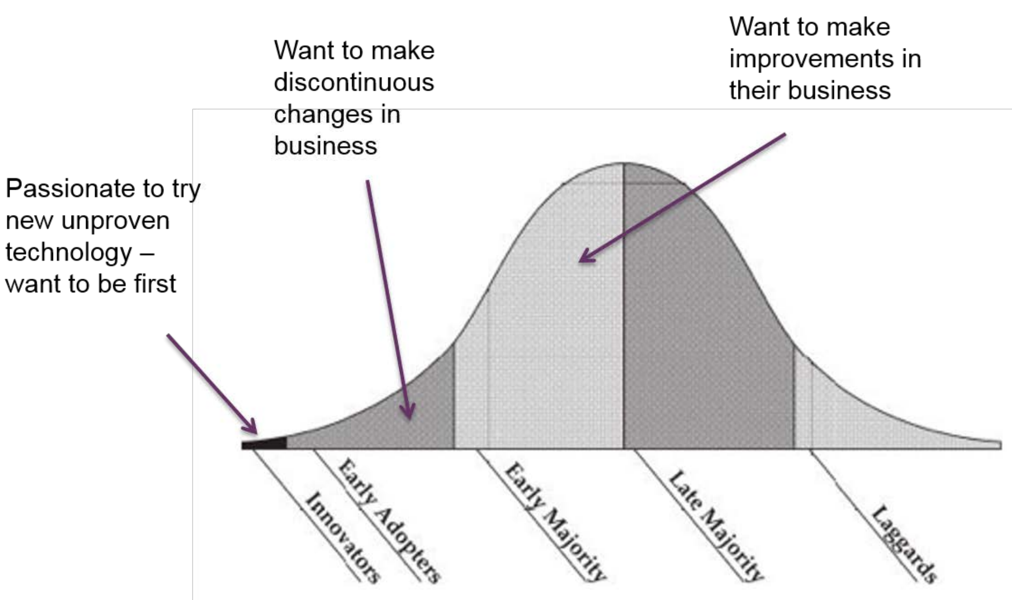

Figure 4-1. Classification of Technology Adopters[6]

[6] From "Crossing the Chasm", 3rd Edition by Geoffrey Moore, 2014.

However, major impact is realized when the MPTs are transitioned to the early majority. A SERC MPT successfully transitioned to the *early majority* would be:

- Widely applied within its potential market of practitioners
- Demonstrably and credibly delivering its intended value when applied
- Widely taught in relevant university programs
- Articulated in books, videos, papers, social media, and other knowledge channels
- Sustained and improved largely by resources and infrastructure outside the SERC, including having commercial quality tooling, training, and a cadre of experts that aid in its application

Once research has been successfully transitioned to the early majority, market and environmental forces are usually sufficient to complete the transition to the late majority and laggards who are usually convinced by the results achieved by the earlier adopters to satisfy their important needs.

As the SERC has continued to grow and mature over the past ten years, the organization has gained significant experience in the area of transition, learning important lessons on what is and is not effective. In addition, the SERC has proactively formed partnerships to strengthen the transition pipeline, building an active network of systems researchers and practitioners. Strong relationships have been forged with several professional organizations, including INCOSE and the National Defense Industrial Association (NDIA) Systems Engineering Division. However, as a research center, the SERC has inherent limitations in the scale at which it can directly support transition. Therefore, the SERC will generally enable and directly support transition only to a small number of *innovators* and *early adopters*. At their discretion, SERC Collaborators may seek to scale MPT transition to a large group of *innovators* or *early adopters* or even seek broader transition of an MPT. Generally, the SERC will play only a very limited or no role in that larger transition. The universities that make up the SERC may take on this role outside of the SERC contract.

Based on past experiences, six principles have emerged that underlie effective transition readiness and progress as shown in Table 4-1. These principles were documented in 2016 and have been applied in varying degrees since the SERC was founded in 2008.

Table 4-1. Six Principles of Successful Transition

Name	Principle
Plan Early	Make successful transition an explicit and well-planned goal from the project's outset, including an early identification of the Stakeholder Community
Balance Long and Short Term	Balance the desire for longer-term higher impact research with the importance of shorter-term utility, incrementally delivering results
Pilot Continuously	Continuously engage both practitioner and student pilot groups to improve the utility and confirm the validity of the research
Engage Community	Build strong engagement with outside communities who can become advocates and adopters
Support Centrally	Strengthen SERC-wide infrastructure and incentives to help projects successfully transition their research
Productize	As adoption scale grows, create mature tools, guides, and other artifacts to help adopters succeed, relying where appropriate on outside organizations that will mature research-grade MPTs into production-quality products and services

As noted, each research project needs to establish a transition plan based on the principles described above. Once this has been completed, the transition readiness of the MPTs resulting from the research needs to be characterized. Two dimensions characterize the ***readiness*** of the MPTs for transition: *relevance* and *practicality*. Relevance is determined by the ability of the new MPT to help Innovators and Early Adopters perform a valuable activity better than they otherwise reasonably could; e.g., does a new approach to understanding the "ilities" of a system architecture really offer relevant insights on reliability, safety, etc. that other MPTs that analyze architectures do not? An MPT has high relevance when it has intrinsically high value and/or differentiating capabilities; e.g., being able to predict with high confidence the cost of building a system of interest or being able to develop an accurate model of the behavior of a system in half the time it would take using other available MPTs.

Practicality is determined by how easily Innovators and Early Adopters can cost-effectively apply it; e.g., is data required for the MPT reasonably available, is automation available to perform the MPT activities, does the MPT work on "real" problems? The bar of acceptability for both relevance and practicality is raised when the MPTs are being transitioned to Early Adopters rather than to Innovators. An MPT has high practicality when practitioners who are skilled in the activity, but not originally skilled in the MPT, can cost-effectively learn it and consistently and cost-effectively apply it to produce valuable results.

Once transition readiness has been characterized for a project or program, corrective actions or improvements can be made based on the transition principles described earlier. However, it is important to measure the transition ***progress*** of the MPT to determine the effectiveness of these measures. Two dimensions can characterize how much a SERC MPT has transitioned to Innovators and Early Adopters: *approval* and *adoption*. Approval is determined by how much better adopting practitioners believe the MPT succeeds at delivering value relative to alternative MPTs. It is the driving force for adoption. An MPT has *high approval* when practitioners routinely praise the MPT's impact, cite evidence of that impact, and advocate for its adoption. Adoption is a measure of how widely the MPT is used by practitioners relative to the potential market of the MPT. An MPT has *high adoption* when practitioners from many diverse organizations use the MPT, it is widely taught in universities, and descriptions of it are available from many sources.

Finally, one of the objectives of this Technical Plan is to help the SERC maintain a healthy diverse research portfolio that supports a steady pipeline of transitioning MPTs. As such, each research project will have a transition plan in place based on a stated set of actions supported by the six transition principles. In addition, each research project will have its transition state characterized based on transition readiness (*relevance* and *practicality*) and its transition progress (*approval* and *adoption*) based on project evidence. This information will provide the SERC and its sponsor the ability to determine the appropriate mix of transition characteristics to support their strategic objectives, to take action when necessary and to provide researchers with the tools to improve their transition effectiveness. Once a research project is complete, those funds become available to invest in other research projects.

5 FOCUS AREAS, PROGRAMS, AND PROJECTS

Since October 2013, every project in the SERC research portfolio has fit into a program in the four Research Areas shown in Figure 3-2. This Technical Plan primarily describes the allocation of Core funds (approximately $5M annually) to existing projects (shown in Figure 5-1) and the potential allocation to new, yet unidentified, projects. However, the SERC research portfolio is much larger and more diverse than would be possible with just Core funding. Between October 1, 2013 and June 1, 2018 more than $38M in cumulative funding has been awarded to SERC projects funded by the Services, Defense Acquisition University (DAU), the IC, and other organizations in the DoD.

Besides directly funding SERC projects, sponsors may provide coordinated funding or in-kind resources that contribute to the execution of SERC projects; e.g., MITRE has coordinated some of its research efforts with tasks in the Systems-Aware Security Project.

Sometimes non-Core funds augment previously existing Core-funded projects e.g., funding contributed by the Intelligence Community towards the Helix Project. At other times, non-Core funds support new projects to which Core funds are later added. Finally, there have been a number of projects spawned by non-Core investment which have no corresponding Core funding, but which help address one or more Missions and/or Research Area Visions.

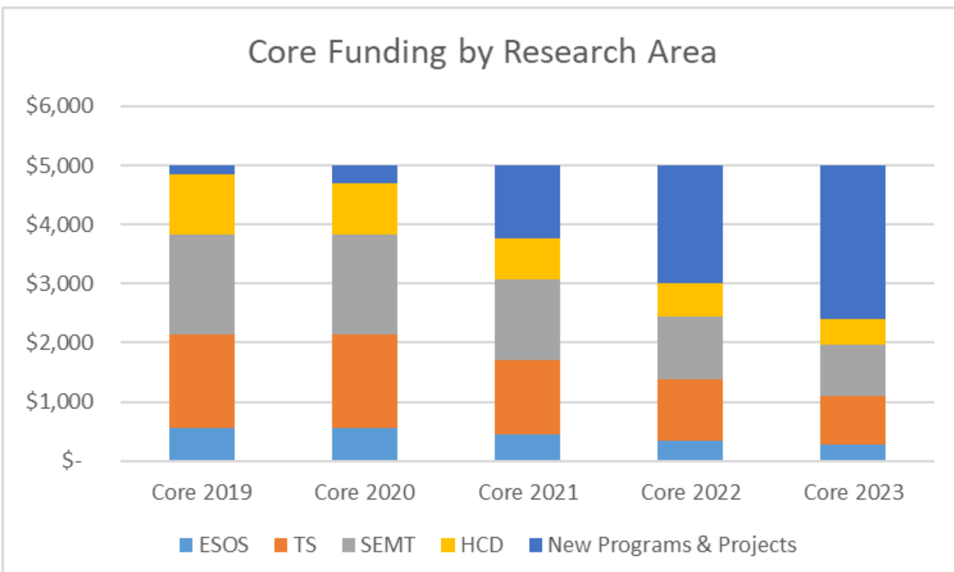

Figure 5-1. Core Funding Distribution across Research Areas

Figure 5-1 shows the anticipated relative distribution of Core funding between the four Research Areas over the five years of the Plan. The general philosophy is that each new project receives steady funding for two years, giving that project time to establish its research approach and begin to obtain early results. Funding for that project is then reduced by 20% annually to incentivize the PI to find funding from non-Core sources. In some cases, projects will end before the five years of this Plan. When projects end earlier than planned, freed up Core funds are accumulated in an investment pool that will be used to fund new programs and projects. This reduction incentivizes researchers to seek additional non-Core funding. For this plan, the SERC is targeting three non-Core dollars for each Core-funded dollar.

Additionally, to encourage PIs to transition their research results into university courses, some Core funds may be allocated for PIs to develop educational materials based on their research results. That material will be shared with all SERC Collaborators and perhaps more broadly. The funding level and timing for this allocation is yet to be determined.

Sections 5.1 through 5.4 describe the Core-funded programs and projects in each of the four Research Areas and provide a short summary of non-Core funded projects in those areas as well. Section 5.5 describes supporting activities that enable the successful execution of these research projects.

5.1 Enterprises and Systems of Systems (ESOS) Research Area

Each DoD/IC Service and Agency, and the larger DoD itself, is an example of an enterprise and these agencies themselves, as well as the products and services they architect and acquire exhibit features of a system of system (SoS): degrees of operational and managerial independence and the propensity to develop emergent behavior. In fact, the literature has offered a variety of types, characterized by the degree of central control and awareness, including: Directed (central authority and funding), Acknowledged, Collaborative, Virtual (systems interact but are not even aware of each other). To this list we add another category, the "fragmented" (systems interact either unaware of each other or in open contention with each and often with significantly conflicted incentives). They are typically fragmented structurally and in terms of budgeting and governance.

Missions include the future conflicts in urban areas and/or that are multi-domain, spanning many or most of the five domains (land, air, sea, space, cyberspace). Further, because of either the urban setting or the expanded cyberspace domain, these conflicts may involve a complex mix of "blue, red, green and gray" elements. Developing capabilities based on the classic red vs. blue planning for this context may no longer apply, as the presence of gray systems which may: a) inadvertently be part of engagement, b) be coopted to serve purposes of red forces, c) create an emergent effect unanticipated by either red or blue. The fact that some of these red, blue, or gray systems may have high degrees of autonomy further exacerbates the challenge of architecting solutions (though offers intriguing new opportunities as well). Methods, tools, and insights are needed to **shape our enterprises**, **architect our SoS capabilities**, and **engineer our missions** with sufficient "velocity" so that their component packages of SoS elements remain effective in rapidly changing environments.

This "comprehensive mission" lens for SoS and Enterprises also brings to the fore the importance to civil/commercial systems whose efficient and adaptable functioning, important in their own right, often have underappreciated importance to defense and security as they lie adjacent to defense/security systems or present vulnerabilities in civil infrastructure systems that underpin our society and way of life. Further, economic factors and policy incentives play a central role in these enterprises, so these factors – and all elements of system behavior—must be part of the research advancement for 'managing' the operation of SoS and Enterprises that own/operate them. Such organizations have the challenge of integrating and evolving multiple portfolios of systems with often-conflicting sets of objectives, constraints, stakeholders, and demands for resources.

5.1.1 ESOS Vision and Current Progress

The ESOS Vision is to:

Create the foundational SE principles and develop the appropriate MPTs to enable the DoD and its partners to model (architect, design, analyze), acquire, evolve (operate, maintain, monitor) and verify complex enterprises and systems of systems to perform mission engineering in a manner that generates an affordable and overwhelming competitive advantage over its current and future adversaries.

The goal to achieve this vision is:

Prototype, demonstrate, and provide MPTs, to transform the development and operational management of end-to-end mission capability (composed of services and platforms with variable autonomy) in complex organizational and mission environments, so those capabilities have fewer unintended negative consequences, quickly recognize and exploit unintended positive consequences, adapt well under changing circumstance, and exhibit greater resilience.

Within this context, research challenges in the ESoS area are centered on:

- Behavioral and social aspects of systems acting within a variety of forms of SoS and enterprises (including ‘fragmented’ ones), and the design of incentives that maximize the probability of the capability outcomes in each particular case
- The use of Autonomy as a “design variable”, to inform mission engineers of which systems should employ which degrees of autonomy from a mission outcome but also from a resiliency perspective, including the exploration of modularity principles in the realm of autonomy allocation
- Analytic processes for understanding goals-plans-scripts-tasks of each human and autonomous component system, as well as information and control requirements for task execution, for the purpose of both aligning performance and identifying inherent conflicts across component systems
- Rapid composition of assets for missions and enterprise-level activities where the consequences of alternative compositions are not well-understand—and how to exploit modular strategies and enable supervisory control by humans in these new compositions
- Managing mission engineering solutions over time as to assess and adapt to behavioral and social changes of the intent, structure, and possibly governance of the system, including instrumenting and monitoring of operational ESoS.
- Identifying the pivot points in mission webs where small changes in capability significantly improve mission outcomes under uncertainty.

Researchers in the ESOS area have made substantial progress towards the required underpinnings of these research challenges, particularly in the ability to model and analyze complex interdependencies and the ability to apply models with case studies to guide operations. Examples include the SoS Analytic Workbench, the completed FILA-SoS body of work, valued-based Kanban scheduling for SoS capability development/enhancement, and the use of enterprise systems modeling (a broader notion than simply multi-level models) demonstrated in the context of counterfeit parts. Some adjacent work in linking SoS cost models to architecture evolution via the Systems Modeling Language (SysML) has also advanced and should be more tightly integrated with other SoS activities for greater impact. Early work in enterprise system models and SysML activities point to the need for even greater effort in visualization and direct tools for decision-support during operations and evolution.

Gaps remain to address the ESOS Vision, especially in the ability of individual systems to understand implications from the SoS architecture and its behaviors. A greater "situational awareness" for key systems, especially in situations of virtual SoS or event fragmented ones, would increase their ability to thrive in the highly dynamic and emergent nature of SoS and Enterprises. Collaborative decision-making tools are promising in this regard. Also, concepts such as quantifying technical debt in existing systems could provide a means for this situational awareness and understanding systems that may support a new or evolved capability. An extension of this gap is the ability to discover and characterize the tension that exists between systems and mission focus. Missions are what warfighters need to accomplish, yet systems are what the DoD develops and acquires. This is a challenge for DoD, as an enterprise, to understand this disconnect and deal with its tensions. The concept of developing SoS capability has advanced understanding of this challenge, but more research is warranted to understand "mission engineering" and its impact on the enterprise.

In addition, although the SoS Analytic Workbench and the counterfeit parts enterprise model have been successfully demonstrated in the SERC Innovation and Demonstration Laboratory (SIDL) (see Section 5.5 for more on this Laboratory), gaps still remain in achieving more ubiquitous and flexible availability to DoD communities. The ESOS Goal requires that the DoD actually use models and tools to make the necessary decisions that lead to superior outcomes. This supports the vision for a form of "SoS Engineering tool repository" that will be hosted in the SERC Innovation and Demonstration Lab (SIDL). Such a repository would identify the right tools available for particular problems and domains, where they can be found, and how they can be used in proper context. While this would not prohibit inventors from advancing and distributing the tools in other ways, a repository with administration by SERC could fill a gap until such tools come to market.

5.1.2 Strategies to Address the ESOS Research Challenges

Successfully executing the following elements of our generic strategy will make significant progress towards addressing the ESOS Research Challenges. All four of the following strategies are integral to the goal for the SERC which includes validation and transition in every research endeavor.

1. *Model:* Develop methods and theories that allow quick and insightful modeling of enterprises/SoSs, in terms of physical, human, economic, and social phenomena, so that the effects of changes in policies, incentives, practices, components, interfaces, and technologies can be uncovered in advance of their implementation

2. *Prototype:* Create prototype mission engineering tools that enable explaining root causes of behaviors and thus provide insight into enterprise/SoS capability acquisition approaches, and the role of individual systems, in the face of significant uncertainty and change to minimize unintended consequences and unforeseen risks

3. *Interactively, Visually Demonstrate:* Conduct exercises with users/practitioners using prototype tools in enterprise/SoS and test hypothesis about abilities to generate insight into different architectural integration and collaboration approaches that facilitate evolution in the face of

uncertainty and change in how an enterprise/SoS is employed, the technologies available to realize it, and the physical, human, economic and social environment in which it exists

4. *Support iterative learning cycles as means of verification: As a philosophy of transition,* support human learning in key outcomes so that they can be monitored and confirmed during development and evolution, especially in experiments that use legacy systems in new ways during operation while development and evolution are underway

In the past, the ESoS area directly implemented these strategies via two research programs: *Enterprise Modeling* and *Systems of Systems Modeling and Analysis*. Given the generic strategy and the common research challenges outlined in Section 5.1.1, going forward these two research programs will be integrated and work together as one multi-pronged thrust, *Comprehensive Enterprise / SoS Modeling and Analysis*, and will pursue the following future tasks described below.

Focus Areas for Future Investigations

- Integration of Service Delivery in Fragmented Organizational Ecosystems, i.e., systems of systems where collaboration cannot be commanded – incentives really matter!
- Behavioral and Social Implications of Autonomy – research into the behavior of system of systems when autonomous collaborators do not have a template for interaction—how to succeed in missions that are more like "pick-up games" with sufficient reliability balance with innovation.
- Deep investigation of how consideration of autonomy and security needs and technologies drive changes in how modularity is considered in both acquisition and engineering design context for both software and hardware and their integration in cyber-physical systems.
- Discovering and characterizing the tension that exists between systems engineering and mission engineering foci. Missions are what warfighters need to accomplish, yet systems are what the DoD develops and acquires. This is a challenge for the DoD, as an enterprise, to understand this disconnect and deal with its tensions.

To advance the integration among present and future activities, the ESOS Area will develop an interest group within the SERC community and develop a Workshop to be conducted in 2019 timeframe to invite all SERC universities into discussion on these envisioned tasks and sponsor community to validate their priority.

Two research programs, described below, directly implement the strategy: *Comprehensive Enterprise / SoS Modeling and Analysis* and *Mission Engineering.*

5.1.3 Comprehensive Enterprise / SoS Modeling and Analysis Program

Almost all definable missions conducted by the US Military are executed via a system of systems--integrating multiple, (semi)-independently managed systems to achieve a unique capability--therefore requiring collaboration and negotiation as well as command and control. Thus, when viewed as involving both the technical systems and their organizational management, mission-engineered SoSs are enterprise challenges as well. Indeed, both enterprises as systems and as SoSs increasingly face situations in which the classical systems approach of deterministically engineering the system based on relatively static requirements and specified human interactions are insufficient. In such complex systems, human behavioral and social phenomena in collaboration are critical as are cascading impacts from interdependencies; altogether, emergent outcomes are the norm. Research is necessary to determine the foundational SE principles for such systems. These principles can then be used to develop associated SE MPTs applicable to such complex systems.

In addition, developing new SoS capabilities while evolving SoSs composition over time to improve performance and stay current with new technologies (e.g., autonomy) remains highly challenging. The complex interdependencies among systems often exhibit managerial and operational independence yet must work cohesively to achieve an overarching set of capabilities. Tradeoffs between capability and risk are essential decisions that must be addressed for SoS capability planning. Existing tools for such tradeoffs are of limited value when size and/or interdependency complexity is high.

This research program addresses the need to create and mature decision-support tools specifically for evolving SoS architectures and capabilities. The research to date has explored analytical methods to quantify the impact of system interdependencies in the context of SoS capability development as well as broader agent models that address the often-fuzzy influence of stakeholder perspectives in the technical development activities. Additional research has focused on identifying innovative approaches to support SE in architecting, engineering, and evolving complex SoS. Continuing research in this area will focus on SoS and constituent system situational awareness, strategic approaches for simplifying SoS architectures and their ability to restructure quickly to respond to new needs and missions, as well as the implementation of an SoS Toolbox repository to make maturing SoSE tools generally available to SoS and constituent system development teams.

Table 5.1-1 offers a description of both projects and which strategies they primarily support.

Table 5.1-1. Projects in the *Comprehensive Enterprise /* SoS *Modeling and Analysis* Program

Project	Started	Purpose	Primary ESOS Supported Strategies
Approaches to Achieve Benefits of Modularity in Defense Acquisition	2016	Identify and prioritize MOSA-related decision-making scenarios for different stakeholders, collect and organize knowledge artifacts regarding best practices, develop a pragmatic decision-support framework guided by the needs of relevant stakeholders identified above	1, 2, 3, 4
Enterprise Systems-of-Systems Model for Digital Thread Enabled Acquisition	2017	Develop a conceptual model of the future DoD Acquisition Enterprise reflecting the transformation to Digital Engineering in the SE process. Using semi-structured interviews, identify agents and enablers/ barriers to change, and metrics/outcomes.	1, 2, 3, 4
Systems of Systems Analytic Workbench	**Completed successfully in 2017**	Develop MPTs and an Analytic Workbench construct to house them for the purpose of SoS architecture analysis, redesign and evolution management	1, 2, 3, 4

5.1.3.1 Approaches to Achieve Benefits of Modularity in Defense Acquisition

SERC *Approaches to Achieve Benefits of Modularity in Defense Acquisition* seeks to develop knowledge artifacts, complemented by a model driven tool, to guide practitioners in making more effective individual and collective decisions related to the modularization and openness of defense acquisitions. The research leverages insights gained from (among others) our prior works, and work funded under SERC *Investigating Approaches to Achieve Modularity Benefits in the Acquisition Ecosystem*, including community driven insights from a MOSA driven workshop conducted under the same prior research effort:

- Researchers shall identify and prioritize MOSA-related decision-making scenarios for different stakeholders, collect and organize knowledge artifacts regarding best practices, develop a pragmatic decision-support framework guided by the needs of relevant stakeholders identified above in the context of relevant processes of the defense acquisition lifecycle, including the evolution of technologies, threats and other strategic factors
- Researchers shall collect and organize knowledge artifacts regarding best practices for the most important MOSA decision scenarios
- Researchers shall develop a pragmatic decision-support framework guided by the needs of relevant stakeholders identified above. The framework should allow stakeholders to:
    - Understand and anticipate technical and programmatic impacts of various modularization (and openness) strategies towards achieving the intended MOSA benefits
    - Explore prefatory tradeoffs between and among common metrics of interest (e.g. cost, schedule, risks) against various strategies for modularization.

Table 5.1-2 shows the focus, deliverables, and investment in the project through 2023.

Table 5.1-2. *Approaches to Achieve Benefits of Modularity in Defense Acquisition* Project Timeline

Year	Focus	Key Deliverables
Pre-2019	Establish the nature and contents of a MOSA Ecosystem Produce initial decision-support framework for MOSA	Initial Program Manager Guidance Document on Leveraging Benefits of MOSA for PMs Initial framework and use case execution with partner programs
2019	Evolved and expanded decision-support framework with trade-off analytics	Use case demonstrations on partner program case studies, to provide evidence of efficacy and trust for program managers
2020	Execute direct MOSA guidance and tool development with programs, and develop final PM Guidance Document	MPTs, Guidance Document, journal articles and software
2021-23	To be determined	To be determined

The *Approaches to Achieve Benefits of Modularity in Defense Acquisition* transition plan and characterization are shown in Tables 5.1-3 and 5.1-4 below.

Table 5.1-3. *Approaches to Achieve Benefits of Modularity in Defense Acquisition* Transition Project Transition Action Plan

#	Transition Action	Principles Implemented
1	Began project with SERC Workshop on MOSA to engage community from the beginning and build network of partners.	• Engage Community • Plan Early

#	Transition Action	Principles Implemented
2	Develop and evolve a "Program Manager's Guide to Achieving benefits to MOSA and Program Success"; initial edition produced at conclusion of project.	• Engage Community • Pilot Continuously Productize
3	Develop a MOSA decision-support framework (DSF) and associated computational tools for PM's to use for learning and exposing key program metric tradeoffs as impacted by modularity and openness	• Plan Early • Pilot Continuously • Productize
4	Leverage partnerships with programs to developed specific relationships with them to produced tailored MOSA decision-support tools that are effective and trusted.	• Productize • Engage Community

Table 5.1-4. *Approaches to Achieve Benefits of Modularity in Defense Acquisition* Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• Responsiveness to feedback from programs on usefulness of MOSA guidance and decision-support tools, especially as the law and policy on MOSA shifts and the emphasis from DOD leadership increases • Adoption, enhancement, and tailoring by programs to reap maximum benefit.
Progress (approval, adoption)	• Conference papers (two already complete), and journal publications (one already published) to establish validation with academic / research community • Feedback from programs that have adopted and enhanced products • Suggested project follow-on activities requested, especially for targeting Mission Engineering applications and use for "new" acquisitions like AI and Autonomy

5.1.3.2 Enterprise Systems-of-Systems Model for Digital Thread Enabled Acquisition

SERC *Enterprise Systems-of-Systems Model for Digital Thread Enabled Acquisition* is analyzing the possible impacts of Digital Engineering (DE) on transformation of the DoD Acquisition Enterprise into a digital and model-based culture. DE is a key enabler for future improvements in acquisition processes and practices. It will allow program managers to reduce both technical and programmatic risk through better interface management and improved understanding of the impact of design choices on cost and schedule. However, it is expected that this impact could reach much further, not only changing the way information is shared in the acquisitions context but fundamentally changing the business eco-system. The transformation from a primarily paper-based set of decision tools to a digital enterprise will likely make a number of current business processes obsolete, change current relationships between the defense acquisition community and the defense industry, adjust roles and associated jobs, and shift stakeholder perspectives on value in the enterprise. One may expect that the various stakeholders will both embrace and oppose transformative changes in ways that maximize their individual values. But, how exactly these complex interactions among stakeholders will affect the acquisitions eco-system is currently not well understood. This research seeks answers to the following questions:

- What changes are likely to emerge from the transition to digital engineering processes, methods, and tools?
- What are the enablers and barriers to such innovation in the DoD acquisition enterprise?
- What stakeholders will be affected and how will they likely embrace or oppose change?
- How might stakeholders be incentivized to embrace innovation and how will this be measured?

- What are the leading and long-term indicators of change?

To answer these questions, the project is using a qualitative research approach using semi-structured interviews of leaders of the DE transition across the DoD and NASA. From the interview narratives, a set of Systemigram models will be created that identify key actors, activities, enablers and barriers to change that drive desired system outcomes. The resulting conceptual model will capture the impact of DE on the emerging model-centric system acquisition process. It will provide a baseline to identify the consequences of DE policies and investments and identify metrics that are critical to acquisition transformation.

Table 5.1-5 shows the focus, deliverables, and investment in the project through 2023.

Table 5.1-5. *Enterprise Systems-of-Systems Model for Digital Thread Enabled Acquisition* Project Timeline

Year	Focus	Key Deliverables
Pre- 2019	Develop conceptual models for the future acquisition process with expected DE transformation.	Initial report containing methods, systemigram models, a futures analysis, and potential change metrics.
2019	Program Office level change strategies, models, and measures.	Develop a service level program office guide to successful DE transition. Develop a set of measurement models that reflect leading indicators and long-term change outcomes at the program office, service level enterprise, and defense engineering/ acquisition/sustainment ecosystem levels. Build a computational model of change drivers.
2020	Engage with and define how the capabilities assessment and development, operational, and test functions can benefit from DE.	Develop rigorous model-based methods to like capabilities assessment and evaluation to program level CONOPS, architectures and requirements.
2021-23	Model curation and certitude, along with metadata standards for the authoritative source of truth. Expansion of DE Use Cases.	A rigorous approach to verify, validate, and accredit the models that are incorporated into the Authoritative Source of Truth. A sustained program that funds the art of the possible in new uses of DE.

The *Enterprise Systems-of-Systems Model for Digital Thread Enabled Acquisition* transition plan and characterization are shown in Tables 5.1-6 and 5.1-7 below.

Table 5.1-6. *Enterprise Systems-of-Systems Model for Digital Thread Enabled Acquisition* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	Transition *Enterprise Systems-of-Systems Model for Digital Thread Enabled Acquisition* developed Systemigrams to an initial Lexicon for Digital Engineering.	• Engage Community

#	Transition Action	Principles Implemented
2	Develop a "Program Office Guide to Successful DE Transition" and associated success metrics.	• Engage Community • Pilot Continuously Productize
3	Develop a computational model of DE transition behaviors that enable understanding of the government/commercial cycles of learning and unique use cases for DE strategies.	• Plan Early • Pilot Continuously • Productize
4	Model the integration of Development and Operational Test processes with the program Authoritative Source of Truth.	• Plan Early • Engage Community

Table 5.1-7. *Enterprise Systems-of-Systems Model for Digital Thread Enabled Acquisition* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• Timeliness with respect to release and implementation of the formal DoD Digital Engineering strategy, immediate use of the project conceptual models (Systemigrams) in DE Lexicon and DE Metrics activities.
Progress (approval, adoption)	• Three conference papers in review, journal publication planned. • Project follow-on activities planned to develop Program Office tools that support successful DE transition.

5.1.4 Mission Engineering Program

Mission Engineering will require two distinct systems engineering toolsets: one will be used in scenario mission planning, and one will be used in the field. The first toolset will answer the question, "What would be the ideal combination of forces, materiel and tactics to achieve the desired effect in this situation?" The second toolset will allow a field commander to explore what can be done with the available assets, including data and digital systems that are continually updated and globally accessible. These toolsets will not only address conventional force projection but will also address the space and cyber warfare domains.

Mission Engineering projects during this period will begin with developing new foundational concepts for Mission Engineering, then work from these concepts to create prototypes of both types of toolsets with plans to transition the prototypes into established DoD software systems. A key thrust will be the utilization of modularity and flexibility to enhance mission effectiveness, and to maintain effectiveness with less forward-based equipment. These projects will naturally connect with work on modular systems in the ESOS research area.

Table 5.1-8 summarizes the projects that were active in 2018 and are candidates for funding in 2019 and beyond.

Table 5.1-8. Projects in the SE Methods Program

Projects	Started	Purpose	Primary SEMT Supported Strategies

PEO Missiles and Space Systems Engineering Methods	2017	Investigate systems engineering methods for weapon systems that are evolutionary in their development process rather than revolutionary.	1

5.1.4.1 PEO Missiles and Space Systems Engineering Methods

This effort was focused primarily on mechanical attributes and was designed to look at the downstream engineering and develop methods of model and data reuse for the typical evolutionary acquisition strategy that Joint Attack Munition Systems (JAMS) Project Office has been following. After identifying the models and data that are used in the downstream engineering, a backwards-planning methodology will be applied to ascertain if there are logical milestones that the model development and data acquisition could be applied to for future acquisitions. If so, this could be the efficient, cost effective path to Future Vertical Lift (FVL) weapons integration.

Table 5.1-9 shows the focus, deliverables and investment in the PEO Missiles and Space Systems Engineering Methods Project through 2023.

Table 5.1-9. *PEO Missiles and Space Systems Engineering Methods* Project Timeline

Year	Focus	Key Deliverables
Pre-2018	Model reuse in evolutionary developments	Bi-monthly and final report
2019	To be determined	To be determined
2020	To be determined	To be determined
2021-23	To be determined	To be determined

The *Transforming Systems Engineering through Model-Centric Engineering* transition action plan and characterization are shown in Tables 5.1-10 and 5.1-11 below.

Table 5.1-10. *PEO Missiles and Space Systems Engineering Methods* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	Implementing Windchill server for non-standard applications	• Pilot Continuously
2	Implementing MagicDraw for non-standard specification development	• Pilot Continuously
3	Model reuse through Analysis Working Group	• Pilot Continuously
4	Model based physical configuration audits (PCA)	• Pilot Continuously

Table 5.1-11. *PEO Missiles and Space Systems Engineering Methods* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• Application to develop non-standard performance-based specification (PBS) from a parent PBS.

Characteristic	Evidence
Progress (approval, adoption)	• Feedback from non-standard community users • Requested feedback from Quality and Production functional areas for model based PCA

5.1.5 ESOS Area Non-Core Funded Projects

At the time of publication, there are no ESOS non-core funded projects.

5.2 Trusted Systems (TS)

The organization of its assets into net-centric systems of systems (NCSOS) has enabled DoD to much more rapidly and effectively see-first, understand-first, act-first, and finish decisively in its operations. However, this implies that each of its assets needs to achieve higher levels of trust as part of the NCSOS, as compared to its previous role as a standalone platform, all the while retaining or improving its previous speed and effectiveness. Achieving those levels of trust is extremely challenging.

The SERC Trusted Systems (TS) research area addresses this challenge, in part, by recognizing the distinction between attributes such as security and resilience as critical system properties while assurance is a process that yields an evidentiary case that a system is trustworthy with respect to the properties its stakeholders legitimately rely upon. This concept is the thread that unifies the prior thematic 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 (i.e., warfighters teaming with these systems to realize the intended capabilities). To provide security, for example, adding protective design patterns to a system (1) can radically alter the overall structure-function holism of the system (2) and may include new machine learning capabilities (3) to achieve those protective design patterns. These themes interrelate, and new methods, processes, and tools for providing assurance that a system is trustworthy must not only be cross-cutting functionally, but also span the full lifecycle and the scenarios in which systems and projects are expected to operate.

5.2.1 TS Vision and Current Progress

The TS Vision is to:

> *Achieve much higher levels of mission trust by applying the systems approach to achieving system assurance and trust for the increasingly complex, dynamic, autonomous, cyber-physical-human net-centric systems and systems of systems.*

The goal to achieve this vision is:

> *Develop, evaluate, and catalyze the transitioning of integrated concepts, methods, processes, and tools for providing cost-effective, evidence-based, argument-supported assurance that defense systems and projects provide all critical properties on which*

diverse stakeholders may legitimately rely for mission success with acceptable levels of residual risk.

The DoD defines system assurance as "the justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle." Trusted Systems consequently encompasses not only the new ways in which these systems are vulnerable to adversarial disruption (Security) but also how these systems behave and hence perform in an operational environment (Function), with increasing levels of interdependencies (Net-Centric Connectedness and Complexity). These are all related aspects; systems will operate as increasingly complex cyber-physical entities themselves, with other systems across heterogeneous capabilities, and alongside human warfighters as well as part of a manned-unmanned team with humans very much in the loop to realize the intended capabilities.

System trust consequently reflects the extent to which one system's assurance is dependent on another system's assurance. In other words, the acceptance of that dependence implies trust between the two. System assurance can only be met through a comprehensive and aggressive systems engineering approach that encompasses the following three critical dimensions: (1) the structure of systems, including architecture, functional architecture, and accounting for various kinds of dynamism for the purpose of resiliency and autonomy, (2) the process and engineering activities by which systems are constructed, evolved, and sustained, including mechanisms for measurement of critical attributes and for management of alternatives and commitments, and (3) the supporting models and techniques through which evidence can be created to support assurance judgments. The SERC's focus has historically been on the last of these three – achieving high levels of trustworthiness – but it is recognized that, moving to meet DoD needs of the near future, a strategic approach is required that builds on the interplay of these three critical dimensions of consideration. This interplay, evident in the diagnosis of assurance failures and root cause analyses, defines the scope of this vision.

The strategy taken across these areas has four principal features: (1) the expression, retention, and analysis of diverse kinds of information related to requirements, design, implementation, and operation; (2) mechanisms whereby the potential consequences of decisions and engineering commitments can be understood as early as possible in the process, including approaches such as iteration, prototyping, modeling and simulation, analytic methods, and other approaches; (3) support for these practices (information management and tight feedback) across the entire lifecycle starting from the earlier stages of requirements formulation and encompassing architecture, design, implementation, evaluation, integration into operating environments and ecosystems, and operation; and (4) ability to respond effectively to changes in the mission operating environment, the SoS context, and the infrastructure environment.

As Digital Engineering and Model-Based Systems Engineering become more prevalent, there is potential to transform traditional system assurance processes to more holistic and more evidence-based forms. The current state of practice in system assurance is in need of a paradigm change. Complexity is reaching a tipping point and the focus on analytic decomposition (identification of component failures) needs to be augmented by approaches that enforce safe behavior (dynamic control). We can no longer 'test in' safety and security, it must be designed in. Assurance must cover any undesired or unplanned event that results in a loss, and address hazards and vulnerabilities as "a system state or set of conditions that, together with worst-case environmental conditions, will lead to a loss."[7] Current assurance methods and tools are all about a half century old, but the technology and system compositions are very different today. There is a recognition of the need for new tools that address the inherent complexity of today's interconnected systems. The four principle features of the systemic assurance strategy are enabled by a digital engineering process. Exploration of model-based strategies for functional design of assurance and for functionally and formally testing these strategies will be a goal of future research in this area.

By way of example, the DoD Cyber Resilient Weapon Systems initiative recognizes that with the cybersecurity threat, individual systems and components cannot be individually assured and trust relationships must be assured with strategies that ensure resilience at the mission level. Analysis of mission level resilience is a core systems engineering need. Research that supports 'designing in' security is needed to address both an assurance problem and a trust problem. The Systemic Security program recognizes that a layered approach from the component level to the mission level is necessary to assure the mission, and this may involve the inclusion of specific threat countermeasures, or design patterns, to assure resilience to cyber-attacks.

With respect to systemic security, this initiative's mainline concept of adding a layer of security through securely monitoring systems for system illogical behaviors that can be assessed as most likely caused by a cyberattack has received significant recognition, both within and outside of the DoD. The approach uses a highly secured Sentinel as both a valuable addition to security and as an economically advantageous system architecture, compared to directly securing the monitored system to a similar level of security as in the Sentinel. In particular, application to physical systems has been seen as an important opportunity for application of this technological approach, as the development and securing of a Sentinel can include elements such as independent sensors and bounded operator control rules as the basis for effective and economical design approaches for detecting attacks. This has resulted in the start of prototyping projects for a DoD radar, a 3D printer (NIST), police cars (Virginia State Police), and an Army/Air Force image exploitation system using a private cloud-based Sentinel.

In the process of conducting this research, two important gaps in the needs for security have been recognized. First, in military operations, individual systems are clustered into SoSs that conduct missions. The missions are the capabilities that need additional security, while the individual systems are the specific means for providing the elements of security. We have seen that in an SoS: (1) attacks can be developed to exploit the seams between individual systems; (2) attacks occurring in a particular system can result in symptoms that appear in another; and (3) defense alternatives of certain mission functions that can be addressed in more than one system can sometimes be much more easily and economically accomplished in one system as compared to another system. This leads to the recognition of the need for better understanding, analysis and design for mission-level security. In 2014-2015 the SERC developed an SoS test bed including multiple ground-target sensor types (video, infrared, acoustic), a radar for airborne targets, an unmanned aerial vehicle, an image exploitation system and a ground defense command and control system. The Secure Mission Laboratory enables the start of a research effort that expands the Sentinel concept to the mission level, including multiple Sentinels providing the basis for managing cyberattacks from a mission perspective. A workshop, initiated through the Naval Cyber Command with Johns Hopkins Applied Physics Laboratory (JHUAPL), was organized to emphasize the need to explore new

[7] Levenson, N. G., and Thomas, J. P. (2018). STPA Handbook. Massachusetts Institute of Technology, March 2018, http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf , accessed June 2018.

concepts for mission level security, with the objective of engaging operational military leaders into the process of mission security requirements, and engaging the technology community into new approaches that more directly relate solutions to mission performance.

Second, the emergence of new DoD initiatives related to highly automated/autonomous systems drives a need for more advanced risk containment technologies. These technologies include both cybersecurity and other technologies that offer resilience that assures continuous system operation. The Sentinel approach has clear overlaps with other risk containment approaches (e.g., fault tolerant design, software assurance solutions), providing an opportunity to integrate these opportunities from (1) a design concept viewpoint, (2) an implementation viewpoint, and (3) in certain cases, from an integrated implementation viewpoint. In addition to technology design issues, other issues related to the role of people in these systems contain significant overlaps as well. This year, the cybersecurity project has included a human factors element, addressing human confidence in responsive decision-making in the event of a cyberattack. The experimental questions being addressed in the human factors project have been seen to overlap with questions faced by the Air Force autonomous systems community at the Air Force Research Laboratory. The Air Force Institute of Technology is engaged with the University of Virginia in addressing the cybersecurity project and is actively evaluating the synergistic opportunities for future research. The SERC anticipates identifying important overlapping interests and defining new project objectives that address the synergistic opportunities.

5.2.2 Strategies to Address the Trusted System Vision

In the face of the disruptive, continuously changing trends relating new system capabilities and vulnerabilities, the TS area aims to promote R&D efforts that lead to enhanced confidence in the achievement of desirable and avoidance of undesirable system properties. Often, these end-state qualities are delivered, in part or in full, by software. With the complexity inherent in current and envisioned systems, as well as their performance as part of an operational system of systems, it is very easy to miss subtle interactions that may lead to highly significant (desirable or undesirable) emergent behaviors and aspects of vulnerability. This is no longer a deterministic, exhaustively tractable problem. Nor is assurance that these systems are trustworthy in terms of their safety and security (key desirable properties, each comprised of many sub-properties) being sufficiently addressed by conceptual understanding and MPT development occurring post-design. To design-in assurance, processes to develop compelling assurance cases must developed alongside the system from its earliest stages of design through its operation in various mission scenarios, which will evolve over time.

Successfully executing the following strategies will make significant progress towards addressing the TS Vision:

1. *Design for System Assurance and Trust:* Develop design patterns and systems architectures (structural and functional), with corresponding systems engineering principles guiding application, and associated design analysis MPTs for early assurance of needed properties.

2. *Understand Assurance of "ilities":* Develop MPTs that promote tangible conceptual understanding and scalable analysis of cost-effective relationships across assurance policies/requirements and "ilities", such as usability, interoperability, and maintainability, comprising reliability, availability, security, etc.

3. *Enable Assessment/Measurement of System Assurance:* Develop MPTs that allow measuring "how much" assurance of needed properties a system has, and that permit comparison of the relative assurance and trust provided by alternative systems.

4. *Understand the Cost of Assurance and Ensure Cost-Effective Assurance:* Develop MPTs that enable understanding, evaluation, prediction to within acceptable levels of risk, and help ensure the cost-effectiveness of implementing high-assurance policies and requirements, especially on complex systems and complex systems of systems.

The TS area's long-term goal is to discover, promote, and support R&D efforts that lead toward *an overarching concept of assurance-driven systems engineering.* The TS thrust will aim to provide foundations for *avoidance of unacceptable losses in defense projects and in operation of defense systems up though the mission level,* whether relevant failures and events are due to natural causes, accidents, or malicious action.

Addressing the evolving, systematic, and comprehensive analysis of threats to trustworthiness requires development and support of research across the entire lifecycle starting from the earlier stages of requirements formulation and encompassing architecture, design, implementation, evaluation, integration into operating environments and ecosystems, and operation. Further, the MPTs produced by this research should embody model-based approaches for functional design and evaluation in keeping with the guiding tenants of the DoD *Digital Engineering* strategy. Recall that, for the SERC, *development* of an MPT includes validation and transition.

Two highly related research programs, each with many research directions underneath and across them, directly implement these four strategies:

- *Systemic Security.* Create, validate, and transition MPTs to ensure systemic security using knowledge of system objectives and operation. Given the numerous sources of security breaches available at low cost to attackers, a major concern is to make DoD systems, SoSs, and enterprises harder to attack, while simultaneously making them more difficult and expensive to penetrate and damage. Ensuring that a system meets its intended security goals is one of the most critical aspects of ensuring that system will perform its intended capabilities as expected in operation. While security is a system property that itself requires assurance, security is also a unique type of vulnerability that did not exist in its current form prior to the technological advances of today's cyber-physical systems. Because of the intense focus security requires, the TS area maintains security as a distinct research thrust while simultaneously recognizing its relationship to *Systemic Assurance*.

- *Systemic Assurance.* Create, validate, and transition MPTs to provide systemic assurance of safety, reliability, availability, maintainability, evolvability, and adaptability The objective of Trusted Systems is to provide assurances that a system will dependably behave as expected and do so without constraining additional functionality or resulting in high-regret, unintended consequences. Increasing automation and the resulting dynamic models of trust and assurance pose key challenges for future systems. Besides security attacks, there are numerous sources of system disruption such as natural disasters, system misuse, system overload, component wear out, and defects in a system's requirements, design, or construction. There are also challenges created through the augmentation of defense systems with increasingly varied levels of autonomy, self-learning, and manned-unmanned teaming. Preventing or otherwise addressing disruptions and untended consequences of these factors, which can cause loss of stakeholders' lives, capability, assets, etc., requires significant improvements in trust not only for current systems, but for the more complex and dynamic DoD systems, SoSs, and enterprises of the future.

A new dimension threading throughout each major area is the concept of assuring *Trusted Resilience.* Resilience is, like complexity, a dynamic and emergent system property. Security is a critical aspect of resilience, as are attributes of autonomy and other system properties; these are not independent. Ensuring systems of the future meet their intended capability objectives requires understanding the interplay across the various system properties and the functional behaviors supported by the development of systems engineering methods and practices to support their analysis. Addressing security requires special treatments that recognize the fact that an adversary creates the events that must be reacted to, and that adversary will consider resilience design features as part of their design of attacks.

The need for more advanced methods to develop evidence-based assurance is additionally driven by the emergence of new DoD initiatives related to highly automated/autonomous systems and manned-unmanned teaming (MUMT). As systems are endowed with varying levels of autonomy, often backed by machine learning, systems engineering approaches must assure the trustworthiness of autonomous behaviors, including methods for partitioning systems into autonomous and human elements to achieve trustworthy behaviors. In addition, formal model-based systems engineering (MBSE) presently encompasses only technical system functionality and capabilities. MUMT functional elements are not well-addressed if at all in the DoD Open Systems (OS) community and are therefore absent from reference and objective architectures. Functional behaviors are required to promote more effective SE practices to identify and characterize MUMT functional behaviors congruent with the formalisms and levels of decomposition already in practice need to be developed, especially for early stages of design. Consequently, the TS area includes these research domains and recognizes that systems with these capabilities require assurance of being both safe and secure. Research must develop data/evidence-driven systems engineering approaches encompassing the expression, retention, and analysis of diverse kinds of information related to requirements, design, implementation, environments, operation, and evolution of these capabilities. Each of these areas will largely fall under Systemic Assurance but will also have aspects under Systemic Security.

In addition, improvements in system trust have been and are being addressed in the other SERC research areas, particularly in SEMT and its current projects: *System Qualities, Interactive Model-Centric SE*, and *Quantitative Technical Risk*. Example contributions from these and earlier SEMT projects include SERC insights such as those from projects addressing technical, integration and manufacturing maturity level assessment, risk management precepts, the enterprise management approach to quantifying early-SE risks, the MIT epoch-era approach to assurance under uncertainty, and the set-based versus point-design approach to assurance of systems undergoing continuing and extensive change. The synergies among these research projects will be addressed and enhanced by periodic cross-research-area workshops.

5.2.3 Systemic Security Program

The goal of the *Systemic Security* Program is to develop MPTs that enable safe, secure, dependable defense systems that are resilient to cyber and other threats through systemic security approaches that complement current, incomplete perimeter/networks. This goal is being achieved by reversing cyber security asymmetry from favoring adversaries (small investment in straightforward cyber exploits upsetting major system capabilities), to favoring the US (small investments for protecting the most critical system functions using systems-aware cyber security solutions that require very complex and high cost exploits to defeat). Building upon the four TS Area strategies to support the TS Vision, the *Systemic Security* strategies are:

1. *Design for System Assurance and Trust*. With an emphasis on designing for system security, develop MPTs that develop solution selections on a mission security basis as opposed to a subsystem basis, recognizing that the interaction between subsystems provides opportunities for adversaries regarding cyberattacks, and also provides potential economies for defenders regarding identification of the most cost-effective way for achieving mission security.

2. *Understand Assurance of "ilities".* Initiate exploration efforts that identify the overlaps and differences between security monitoring as employed in the Systems-Aware concept and performance monitoring for autonomy, recognizing that autonomous systems will need to include monitoring functions for performance assurance. This will require understanding how autonomous capabilities relate to system properties, with inherent degrees of variation, and the "ilities" including but not limited to reliability, availability, security, etc.

3. *Enable Assessment/Measurement of System Assurance.* Develop design patterns and security architectures that enable security to be based on the specific properties of the system and its implementation as a complement to traditional perimeter strategies. Develop methods to comparatively assess and measure how these patterns change system properties and consequently impact assurance and development of assurance use cases. Address security of weapon systems, sensor systems, physical plant systems as well as IT systems within the context of SoSs applied to military missions; e.g., air defense, point target defense, and warning systems. Account for operational procedures and human factors in the SoS context.

4. *Understand the Cost of Assurance and Ensure Cost-Effective Assurance.* Support security requirements assessments that directly address cost and achievement of cost-effective security by developing MPTs that enable understanding, predicting, and ensuring the cost-effectiveness of implementing specific security policies and requirements, especially on complex systems and complex systems of systems

This research program implements all four TS strategies above. Table 5.2-1 offers a description of the two projects currently underway in this program and the strategies they primarily support.

Table 5.2-1. Projects in the Systemic Security Program

Project	Started	Purpose	Primary TS Supported Strategies
Systems-Aware Security	2011	Develop and then refine Systems-Aware MPTs and pilot them in multiple application areas	1, 2, 3, 4
Systemic Security and the Role of Heterarchical Design in Cyber-Physical Systems	2018	Investigate functional modeling of cyber-attacks and countermeasures as a directed graph supportive of simulation to reveal behavioral dynamics across the CPS, threat, and protection elements for design decisions.	1, 4

5.2.3.1 Systems-Aware Security Project

In 2011, SERC *Systems-Aware Security* developed a rapid prototype security capability that includes (1) data continuity checking within the application, (2) real-time virtual configuration hopping of selected command and control functions across multiple operating systems to provide defense through diversity, (3) real-time physical configuration hopping to both provide defense through diversity and resilience in the face of successful attacks, and (4) a closed loop control system for automatic restoration from a successful attack. In 2012-2013, SERC *Security Engineering Pilot* developed a prototype flight-capable security capability directed toward an unmanned air vehicle (Outlaw aircraft containing an embedded Piccolo flight control system) carrying a pre-existing set of surveillance equipment (video/infrared cameras, radar, and a signals intelligence package).

Follow-on activities have been primarily funded by external agencies but will be summarized here. Efforts through 2018 in System Aware Cybersecurity extended the research to focus on resilience features that sustain operator control of weapon systems and assure the validity of the most critical data elements required for weapon control. The decision support tool research focused on integrating historical threat considerations as well as risk considerations into the planning for defenses. Specifically, research investigated the threat analysis aspects of the integrated risk/threat decision support process and included the development of new threat analysis methods focused on mission-aware security. The principal goal was to create and update decision support tools to help decision-makers understand the relative value of alternative defense measures.

The evaluation efforts regarding algorithms for enhanced automation for decision support reached a transitionable state. Development continued on a first prototype of the hardware, software, and operational emulation of the weapon system to be evaluated by use of the decision-support tools. The 'War Room' approach to threat analysis yields SysML representations that both (a) capture mission objectives and system behavior while (b) providing a representative surrogate surface for attack tree application. The team developed both the methodology and associated toolset with the explicit intention of generality and broad applicability. Development is complete on a first prototype of a hardware/software emulation weapon system (referred to as Silverfish) created for testing the decision-support tools. The system includes emulation of all major components of an actual weapon system while also allowing the exploration of more complex operational scenarios and attack spaces, including system-of-systems operations and attacks.

The team made significant progress on developing the architectural decision support tools. The analysis and modeling methodology take a mission-centric viewpoint, combining inputs from system experts at the design and user levels utilizing Systems-Theoretic Accident Model and Process (STAMP) to identify potentially hazardous states that a system can enter and reason about how transitioning into those states can be prevented. The SysML Parser tool was developed that connects general system descriptions with a graph model of the system that can be 'virtually attacked' by a cyber analyst using the Cyber Analyst Dashboard tools. Research in 2018 included developing a deeper understanding of open source cyber-attack databases (e.g., CAPEC, CWE, CERT, and CVE), as well as defining and developing SysML modeling constructs and a traceability ontology to effectively capture relations between missions and system components in the presence of attack patterns. Key accomplishments for this phase include: (1) use of several different querying techniques to characterize relationships between attack classes in CAPEC, CWE, and CVE; (2) refinement of a GraphML meta-model; (3) development of a CYBOK (Cyber Model of Knowledge) model to determine which information from the cyber domain needs to be present in the SysML mission-aware model; and (4) development of the Cyber Analyst Dashboard. The dashboard presents an interactive view of both the 'System' and the 'Attack Space' and allows for several different levels of automation as well as human/analyst interaction.

Table 5.2-2 shows the focus, deliverables, and investment in the project through 2023.

Table 5.2-2. *Systems-Aware Security* Project Timeline

Year	Focus	Key Deliverables
Pre-2019	Development of an end-to-end process for capturing security related mission requirements and evaluating cyber resilience. Develop and demonstrate a secure sentinel function that monitors system behaviors for cyber-attacks.	Prototype solutions that demonstrate readiness for transition to application
2019	Expand the requirements development methodology to include test and evaluation and human factors considerations. Develop other use cases beyond military weapon systems	Initiate preparation of SE processes to provide high quality and efficient methodologies for development of resilient systems
2020	Provide support for an initial transition project	To be determined
2021-23	To be determined	To be determined

The *Systems-Aware Security* Project transition action plan and characterization are shown in Tables 5.2-3 and 5.2-4 below.

Table 5.2-3. *Systems-Aware Security* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	Initiated collaboration with Navy 10th Fleet (Cyber Command) and JHUAPL in addressing requirements methodology and support tools, including organizing a workshop to introduce the research to them. Met with large Aegis Program Manager group to engage their interest.	• Plan Early • Engage Community
2	The University of Virginia has licensed Systems-Aware technology to a start-up company (MSI) engaging in offering new security products and services related to Systems-Aware concept and have initiated efforts to gain new patents.	• Engage Community • Pilot Continuously • Productize
3	Integrated AIMES prototype into a live prototype SoS environment to highlight mission-oriented approach to security including an operational system.	• Engage Community • Pilot Continuously • Productize
4	Initiated projects with NIST on 3D Printers and Virginia State Police focused on automobiles that have both provided confirmation of potential value and provided new elements of learning for transition into military systems.	• Engage Community • Pilot Continuously • Productize
5	Included Air Force Institute of Technology as part of the Human Factors research efforts.	• Engage Community

#	Transition Action	Principles Implemented
6	Involved the DoD Chief Information Officer in the definition of the Cloud computing portion of the project.	• Plan Early • Engage Community
7	Involved the Deputy Assistant Secretary of Defense for Emerging Capability and Prototyping) in supporting the definition of a rapid prototyping project that is directed toward development of an operational prototype radar system with System Aware security capabilities.	• Plan Early • Engage Community

Table 5.2-4. *Systems-Aware Security* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• Application to existing Army/Air Force AIMES system, etc.
Progress (approval, adoption)	• The project has published 5 journal articles with one currently under review, 4 conference papers, 4 technical reports, and numerous public presentations. • Air Force, Navy, DoD Chief Information Officer are engaged in project efforts; MITRE, SEI have provided support to the project • Through the Virginia Cybersecurity Commission, have initiated an economic development plan that addresses support for education and research activities that bring together the cyber-physical systems community with the cybersecurity community

5.2.3.2 Systemic Security and the Role of Heterarchical Design in Cyber-Physical Systems

Defense systems in operation and development today are increasingly what we call cyberphysical in nature. Cyberphysical systems (CPS) combine sensors and actuators to perceive and act in the physical world with communication to enable information, data flow and computation to drive decision making and control the physical actuation. While CPS offer the potential for tremendous new capabilities, their 'cyber-ized' computation and communication backbone coupled with readily available technological advances makes them vulnerable to classes of threats previously not relevant for many defense systems. Cyberattacks are now a tremendous concern for the future of military operations, and this has spawned a drive to intentionally design "cyber resilience" into these systems at the early stages in ways that are amenable to comparative analysis and verification within the systems engineering process. Recent studies from Rand[8] and a 2016 Defense Science Board[9] are especially relevant to the design and evolution of CPS for defense. Both noted similar limitations in current processes, namely that current policies, guidance, and practice still assume stable and predictable operational environments and lack methods to consider the dynamics between rapidly changing threats and system configurations.

The overarching goal of the proposed research program is to advance the theory and practice of systems security design and analysis for cyberphysical systems in ways that will specifically address the concerns

[8] Snyder, D., Powers, J. D., Bodine-Baron, E., Fox, B., Kendrick, L., & Powell, M. H. (2015). Improving the cybersecurity of US Air Force military systems throughout their life cycles. RAND Corporation, Air Force Project, Santa Monica, CA.

[9] Defense Science Board (September 2016). Task force report on Cyber Defense Management. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, DTIC number AD1023639.

noted above. We distinguish security from the broader concept of resilience in that security focusses on protecting defense systems from sentient adversaries. Cyber systems are generally designed by initially specifying critical and other necessary functionality. The high-level functionality is decomposed into specific functional capabilities, and system requirements derive from these functional needs. Boehm and Kukreja[10] distinguish between functional and non-functional requirements as what the system does and how well it does those things, respectively. The –ilities, or system qualities (SQs) of a system such as maintainability, changeability, survivability, etc. are best understood through their relation to the non-functional (i.e., performance) requirements. From this perspective, security is another non-functional quality. Security is assessed based on how well a given security design pattern protects the system as intended – while sufficiently sustaining the critical functional capabilities.

Table 5.2-5 shows the focus, deliverables, and investment in the project through 2023.

Table 5.2-5. *Systemic Security and the Role of Heterarchical Design in Cyber-Physical Systems* Project Timeline

Year	Focus	Key Deliverables
Pre- 2019	Assess the current state of education in U.S. universities related to engineering secure cyber-physical systems and develop initial curriculum guidance.	The initial report developed a taxonomy for CPS security, a survey of education against that taxonomy, initial mapping of competencies and curricula, and an example professional development course.
2019	Develop a framework addressing people, roles, processes, and outcomes for successful System Security Engineering (SSE). Develop a training lab in this domain.	A lexicon that combines foundational principles of dependable and secure computing with DoD missions, and a competency framework for SSE professionals in the weapon system domain.
2020	Best practices and tailoring of the NIST 800-160 SSE guidance for use on development and acquisition programs.	A best practices guide. Detailed process guides for designing in security. Support for a reference curricula in this domain.
2021-23	Application of best practices and competency development to large programs.	Methods to model the attacker/defender space rigorously in early stage system analysis to build more robust processes for building and pruning attack analyses.

The *Systemic Security and the Role of Heterarchical Design in Cyber-Physical* transition plan and characterization are shown in Tables 5.2-6 and 5.2-7 below.

Table 5.2-6. *Systemic Security and the Role of Heterarchical Design in Cyber-Physical* Transition Project Transition Action Plan

#	Transition Action	Principles Implemented
1	Transition the report outcomes to the DoD Cyber Resilient Weapon Systems Community of Interest.	• Engage Community

[10] Boehm, B., and Kukreja, N. (2015). An Initial Ontology for System Qualities. In INCOSE International Symposium, vol. 25, no. 1, pp. 341-356.

#	Transition Action	Principles Implemented
2	Develop and deliver a robust competency framework for the development of System Security Engineers.	• Engage Community • Pilot Continuously
3	Develop a best practice guide for implementation of NIST 800-160.	• Engage Community • Pilot Continuously

Table 5.2-7. *Systemic Security and the Role of Heterarchical Design in Cyber-Physical* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• Initial results were used to and well received in a DoD workshop to engage government, industry, and academia in discussion of CPS security education.
Progress (approval, adoption)	• An initial program on cyber-attack resilient cyber physical systems was provided by UVA to the Defense Intelligence Agency and derivative programs are currently under consideration by the Navy and Air Force.

5.2.4 Systemic Assurance Program

Besides security, the engineering of resilient DoD systems requires assurance of safety, reliability, availability, durability, survivability, maintainability, evolvability, adaptability, and sustainability. Systems cannot be deployed until customer organizations judge them fit for use in the mission environment. These assurance judgments must be based on evidence that a system manifests not just the necessary functionality but also these quality attributes, and at a level appropriate to the operating environment. All of this assurance needs to be achieved for increasingly complex, dynamic, cyber-physical-human net-centric systems, SoSs and enterprises with needs for rapid response incompatible with most heavyweight assurance MPTs.

Research in the last period surveyed the systemic assurance landscape. Research in systemic assurance is expected to grow in the near future with the DoD focus on Resilient Cyber-Physical Systems and the need to design in assurance for both safety and security in a cyber-enabled mission space. In December 2017, the two-day workshop on Model-Based System Assurance (MBSA) explored top-priority research projects for next-generation system assurance design and test, developing a shared understanding of challenges, opportunities and ideas on this topic area. Two prioritized research directions were identified: 1) the need to do an MBSA Pilot with cyber resilience focus, which would be to push the tools and pioneer the processes for functional design in the assurance domain; and 2) the need for better leveraging existing formal methods and techniques from the software engineering community, and enabling their integration with functional models, executable models, and simulation models from the system engineering community, in order to achieve the benefits of model reuse and integration to address MBSA challenges.

All four of the new incubator projects are targeted at the systemic assurance project, and a new research task to begin the MBSA pilot development is being defined. Table 5.2-8 below offers a description of the projects that are currently active in this program area.

Table 5.2-8. Projects in the *Systemic Assurance* Program

Project	Start	Purpose	Primary TS Supported Strategies
Identifying and Measuring Modularity Violations in Cyber-Physical Systems	2018	Develop techniques, metrics, and models that would allow stakeholders to detect, measure, and understand modularity violations in developed and acquired cyber-physical systems.	1, 3, 4
Data Science Approaches to Prevent Failures in Systems Engineering	2018	Develop automated ways of tracking risk that are based on the real reasons of systems engineering failures using existing data and "wisdom of the crowd" indicators.	2, 3
Game-theoretic Risk Assessment for Distributed Systems (GRADS)	2018	Investigate strategic design games and measures of risk dominance to assess inherent risks in decentralized architectures.	1, 3, 4
Human Machine Team (HMT) Concepts for Resilient Autonomous Systems	2018	Develop a methodology for organizing and evaluating the results of human-in-the-loop experiments to understand the importance of selecting the most robust HMT solutions and their characteristics. Develop reusable approaches for design of operational test and evaluation processes to support system developments.	3, 4

5.2.4.1 Identifying and Measuring Modularity Violations in Cyber-Physical Systems

The term "cyber-physical systems" emerged around 2006, when it was coined by Helen Gill at the National Science Foundation. Gill defined a cyber-physical system (CPS) as an integration of computation with physical processes. However, one of the challenges to designing and managing cyber-physical systems is that there are techniques to represent either the cyber processes or the physical processes, but not both. From the "cyber" perspective, there are different techniques to represent the architecture of software systems, such as architecture description languages, UML models, and component models. From the physical perspective, there are different traditional engineering techniques to model the development of physical systems. However, there are some instances of research that take a more holistic approach to architecting cyber-physical systems.

What all of the above have in common is a focus on designing cyber-physical systems to be modular. However, there is no guarantee that the realized system will exhibit the intended modularity. The need to assess the actual modularity of a cyber-physical system is particularly acute. As Lee points out[11], Cyber-physical systems have always been held to a higher reliability and predictability standard than general-purpose computing. Without reliability and predictability, cyber-physical systems will not be applied in safety-critical domains like traffic control, automotive safety, and healthcare. While a modular design is just one approach to improve reliability, predictability, and maintainability; when it is employed, one would like to know how well it was achieved. While approaches to assess modularity in pure software systems have been developed, to the best of the investigators' knowledge no approaches have been developed that specifically address the unique challenges of assessing the modularity of cyber-physical

[11] Lee, E. A. (2008, May). Cyber physical systems: Design challenges. In Object oriented real-time distributed computing (isorc), 2008 11th ieee international symposium on (pp. 363-369). IEEE.

systems. Thus, the question is whether existing approaches from the software domain can be adapted to the cyber-physical domain.

Table 5.2-9 shows the focus, deliverables, and investment in the project through 2023.

Table 5.2-9. *Identifying and Measuring Modularity Violations in Cyber-Physical Systems* Project Timeline

Year	Focus	Key Deliverables
Pre- 2019	• Perform initial feasibility study using software related data to imply hardware related modularity violations in cyber-physical systems	• Technical report disseminated under New Project Incubator • Technical paper published and presented at CESUN 2018
2019	• Explore different criteria to decompose a complex Cyber-physical system into modular structure of different granularity • Build domain concept learner to help identify hardware related modularity violations in cyber-physical systems	• Scholarly paper(s) introducing the approach to identify and measure modularity violations in cyber-physical systems • A proof-of-concept demonstrator to show how to identify and measure modularity violations in cyber-physical systems
2020	• Conduct extended case studies based on research methodology built earlier for identifying and measuring modularity violations and for providing diverse redundant solutions for detected cyber-attack caused failures of critical system modules	• Technical reports discussing the general applicability of research methodology on different subjects • Improved working prototype of useable tools
2021-23	• Transition research methodology to practice by working with real cyber-physical systems in acquisition field	• Technical reports or research papers discussing the effectiveness of the research methodology for modularity violation detection

The *Identifying and Measuring Modularity Violations in Cyber-Physical Systems* transition plan and characterization are shown in Tables 5.2-10 and 5.2-11 below.

Table 5.2-10. *Identifying and Measuring Modularity Violations in Cyber-Physical Systems* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	Project selected in competitive process for New Project Incubator to perform a feasibility study and reduce research risk	• Engage Community • Plan Early
2	Intermediate results presented at SERC Advisory Board Meeting, SERC Incubator Day, and SERC Sponsored Research Review to receive feedback	• Engage Community • Conduct empirical study
3	Research paper published and presented at 7th International Engineering Systems Symposium	• Engage Community
4	Research deliverables include scholarly papers and proof-of-concept tool demonstrator	• Engage Community • Support Centrally • Productize

Table 5.2-11. *Identifying and Measuring Modularity Violations in Cyber-Physical Systems* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• Preliminary empirical case studies on real cyber-physical systems: OpenWrt and MD PnP • One scholarly paper published and presented at CESUN conference
Progress (approval, adoption)	• In-depth empirical case studies on real cyber-physical systems: OpenWrt and MD PnP • General approach for identifying and measuring modularity violations in cyber-physical systems • Development of proof-of-concept tool

5.2.4.2 Data Science Approaches to Prevent Failures in Systems Engineering

Anecdotes and statistics on the failures of systems engineering have become a sure-fire way of attracting attention and lamentation during presentations. No one is immune to the failure disease and in particular past success is no guarantee of future performance - organizations that have succeeded spectacularly in one project may fail just as spectacularly in the next project. In response to these dire statistics, new methods, processes, and tools are continuously proposed and implemented, including numerous new methods of risk identification, tracking, and management. Yet the frequency of failures shows no signs of decreasing, and, meanwhile, engineering creativity in large complex systems seems to be stifled. Rather than the revolutionary creations our 20th century counterparts foresaw appearing in the 21st century, we have limited ourselves to evolutionary improvements.

Why do these methods not help as much as we hoped? One possible reason is the reliance on extensive data creation, collection, and tracking. When projects are under pressure, activities that are seen as non-essential to the core task will not be performed, or, worse, will be performed in a cursory compliance-oriented fashion, potentially leading to misleading data and erroneous conclusions about the state of risk. What if we could, instead, do all this risk tracking and reporting with existing information? Our proposed effort leverages two main ideas: (1) risk assessment based on the “real reasons” for systems engineering failures, and (2) combining existing data with Wisdom of the Crowd (WoC) indicators to uncover the correlations between various (unreliable) traditional and crowd-derived measures, and the measurable outcome (success, failure, or delay). We intend to develop a tool to help organizations track and manage the risks of project failures. The tool is built around state-of-the-art relational deep learning together with contextual bandit techniques, using a combination of enterprise data, and “Wisdom of the Crowds” data that employees enter into a mobile device app. The code is continually refined using each organization’s own data.

Table 5.2-12 shows the focus, deliverables, and investment in the project through 2023.

Table 5.2-12. *Data Science Approaches to Prevent Failures in Systems Engineering* Project Timeline

Year	Focus	Key Deliverables
Pre- 2019	To collect crowd data from a range of student engineering design projects and develop a first generation of the risk prediction machine learning algorithm trained on these data.	Initial report containing sets of crowd signals and associated factors, an initial version of the machine learning software, and IRB-approved protocols for the study.

Year	Focus	Key Deliverables
2019	To refine and expand the data collection process, detect mechanisms between particular failures and causal factors, and create a prototype version of the Wisdom of the Crowd app that collects input data and displays risk predictions.	Sets of tables that reveal causal mechanisms between factors and failures or project outcome, a prototype version of the data collection and prediction app, and a final version of the machine learning software.
2020	To evaluate the usefulness of the risk tracking and prediction methodology in one or ideally two engineering organizations	Technical report containing employee input signals and associated project failures observed in organizations.
2021-23	Assuming previous steps are successful, refine and potentially commercialize the tracking tool.	Technical report describing the necessary steps to create a professional version of the risk prediction tool and associated software.

The *Data Science Approaches to Prevent Failures in Systems Engineering* transition plan and characterization are shown in Tables 5.2-13 and 5.2-14 below.

Table 5.2-13. *Data Science Approaches to Prevent Failures in Systems Engineering* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	Submitted IRB protocols before initiating data collection that will cover student projects university-wide and not restricted to engineering	• Plan Early
2	Continuous adjustment of input data collection approach while expanding collection to more student projects and departments for next collection cycles. Discuss with instructors the potential of collecting project data in more courses.	• Plan Early • Pilot Continuously
3	Creation of a risk prediction environment to encompass the Wisdom-of-the-Crowd input data app and machine learning algorithms.	• Productize
4	Contact partner organizations (federal and private) to collect data and investigate the applicability of the research	• Pilot Continuously • Engage Community

Table 5.2-14. *Data Science Approaches to Prevent Failures in Systems Engineering* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• Initial concept and plan were presented at the 2017 SSRR meeting and were well received by attendees.
Progress (approval, adoption)	• Approved IRB protocols that will cover the data collection in student projects university-wide • Planned an initial conference publication with a trial data collection of student projects in one course

5.2.4.3 Game-theoretic Risk Assessment for Distributed Systems (GRADS)

Sustained interest in distributed system architectures presents an important tradeoff in conceptual design. Distributed systems pursue superior performance compared to traditional monolithic systems through greater flexibility, robustness, and efficiency. For example, arguments for fractionated spacecraft systems emphasize elements of architectural flexibility in uncertain contexts as more information is gathered in operations, risk diversification across multiple systems, spatial distribution to mitigate failures or attacks, and lower cost for individual components. Similar arguments in the decentralization theorem in economics argues distributed systems can exhibit finer control to more efficiently match available resources with localized demands. However, by definition, distributed architectures also introduce new interdependencies between constituent modules which can lead to overall system failure if not understood or anticipated. These effects are amplified by communication barriers if constituent systems are owned and operated by independent entities as a system-of-systems or federation-of-systems. In infrastructure, for example, cross-sector interdependencies can directly lead to cascading failures and loss of critical societal functions. This paradoxical relationship has been described as "robust yet fragile" in systems literature and highlights a fundamental tradeoff between risk and reward which remains a critical area of research in systems engineering.

Engineers and decision-makers must understand the tradeoffs associated with alternative system architectures during early conceptual design activities to best inform concept selection and detailed design. However, the current approach of treating systems engineering as a centralized decision-making process is not appropriate for distributed system architectures due to the inherent lack of control. Applying existing value-centric and tradespace exploration methods to distributed systems only emphasizes the positive upsides of collective action and provides little analysis of the strategic incentives among interactive decision-makers. The objective of this project is to develop and evaluate a game-theoretic risk dominance metric and assessment method to compare monolithic and distributed system alternatives in the context of multi-architecture tradespace exploration. Grogan et al.[12] showed how federated systems—one type of distributed system—can be modeled as a Stag Hunt game where an independent (centralized) design is analogous to a payoff dominated equilibrium and a federated (distributed) design is analogous to a payoff dominant equilibrium. Results showed how Selten's[13] weighted average log measure (WALM) can assess strategic risk for two-player cases and demonstrated why the payoff-maximizing alternative may not be the most desirable choice. This project seeks to extend and demonstrate game-theoretic risk assessment approaches and, particularly, investigate how risk dominance measures similar to Selten's WALM can evaluate alternative architectures in more general design cases.

Table 5.2-15 shows the focus, deliverables, and investment in the project through 2023.

Table 5.2-15. *Game-theoretic Risk Assessment for Distributed Systems (GRADS)* Project Timeline

Year	Focus	Key Deliverables
Pre- 2018	• Perform initial feasibility study of game-theoretic measures for asymmetric games with more than two players	• Technical report disseminated under New Project Incubator

[12] Grogan, P.T., K. Ho, A. Golkar, and O.L. de Weck (2018). "Multi-actor Value Modeling for Federated Systems," *IEEE Systems Journal*, 12(2):1193-1202.

[13] Selten, R. (1995). "An Axiomatic Theory of a Risk Dominance Measure for Bipolar Games with Linear Incentives," Games and Economic Behavior, 8(1):213-263.

Year	Focus	Key Deliverables
2019	• Refine systems engineering and design methodology to evaluate point design concepts using game-theoretic measures • Demonstrate use of game-theoretic measures in application case similar to National Polar-orbiting Operational Environmental Satellite System (NPOESS)	• Scholarly paper(s) introducing overall design methodology and documenting results of validation case study • Supporting computational scripts to calculate and visualize game-theoretic metrics
2020	• Extend systems engineering and design methodology using game-theoretic measures to evaluate design trade spaces • Demonstrate use of game-theoretic measures in extended application case based on distributed or federated space systems	• Scholarly paper(s) discussing overall design methodology and documenting results of validation case study
2021-23	• Transition design methodology to practice by working in concert with a prospective development or acquisition project	• Technical reports and/or scholarly papers discussing application of design methodology to prospective projects

The *Game-theoretic Risk Assessment for Distributed Systems (GRADS)* transition plan and characterization are shown in Tables 5.2-16 and 5.2-17 below.

Table 5.2-16. *Game-theoretic Risk Assessment for Distributed Systems (GRADS)* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	Project selected in competitive process for New Project Incubator to perform an initial feasibility study and reduce risk for a dedicated research task	• Engage Community • Plan Early
2	Intermediate results presented at SERC Advisory Board Meeting, SERC Incubator Day, and SERC Sponsored Research Review to receive feedback	• Engage Community • Pilot Continuously
3	Targeted application case scenario leverages an existing case study analyzed within the Department of Defense and NASA Earth Sciences Division	• Engage Community • Support Centrally
4	Research deliverables include scholarly papers and computational artifacts to help transition fundamental knowledge to academic and practitioner audience	• Engage Community • Productize

Table 5.2-17. *Game-theoretic Risk Assessment for Distributed Systems (GRADS)* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• Distributed or federated systems are a topic of active discussion across multiple levels of the federal government but not well-characterized by existing design methods and tools • Formulation of a game-theoretic metric enables a rapid assessment of strategic dynamics to inform decision-making in proposed joint or collaborative projects

Characteristic	Evidence
Progress (approval, adoption)	• One journal publication in review • Initial engagement with the NASA Earth Sciences Division to synergize research topics

5.2.4.4 Human Machine Team (HMT) Concepts for Resilient Autonomous Systems

The research effort described in this section addresses critical issues related to defining the roles of operators of resilient military systems regarding continuation of operations in the face of significant disruptions through use of cyberattack or other non-kinetic techniques. Prior SERC research activities have focused on automation for detecting such adversarial cyberattack tactics and have explored system resiliency concepts for providing autonomous system reconfiguration responses that rapidly reconstitute proper system operation. The current gap in this line of research endeavors is *the undefined role of human operators* in providing mission-context-driven solutions, through collaboration with autonomous agents *as a Human-Machine team.* The derivation of these resiliency solutions must account for how the autonomous system interacts with other systems engaged in carrying out the overall desired mission.

The broad conclusion to be drawn from past research efforts is that achieving resilience regarding the conduct of military missions that employ autonomous systems will require development of *robust* (i.e., relatively insensitive to possible violations in the method's required assumptions or rules) *human-machine team (HMT) concepts*. The derivation, selection and validation of HMT solutions will require the conduct of human-in-the-loop experiments and operational exercises that involve adversaries successfully corrupting autonomous system capabilities that support missions of concern. The Air Force has developed a wide range of experimental protocols and simulation methods to evaluate and implement decision-support systems. However, current autonomous systems are not built with cybersecurity considerations taken into account, and a new framework to support human-in-the-loop experiments that involve cyberattacks and defense for assessment is needed.

For resilient HMT solutions, a reconfigurable system architecture needs to be flexibly distributed between operators and autonomous agents in response to the mission context. This purpose of *"adjustable" autonomy includes a sequence of processes to represent, measure, distribute, and evaluate performance in a human-machine team*. Of particular concern with this team performance is the variability of operators' decision making under dynamically-changing environments when rare instance of cyberattacks occur. A vast body of literature has attempted to explain this variability, with emphasis on behaviors, cognition, perception, or adaptation. An engineering approach for designing the military operator's decision responses to cyberattacks and subsequent reconfiguration process that can be accomplished within the time constants provided for other aspects of system development is a critical challenge of the current project.

For each attack scenario in the proposed experiment, multiple technical reconfiguration solutions can be derived, each accompanied by a set of possible HMT solutions. In order to understand the importance of selecting the most robust HMT solutions and their characteristics, this project will develop a methodology for organizing and evaluating the results of human-in-the-loop experiments. The initial version of the methodology will be determined based upon the results of conducting a case study focused on a mission whose performance can potentially be adversely impacted by enemy attacks (non-kinetic). This first use case will be evaluated through high fidelity experiments from the viewpoint of combined operator/autonomous system HMT performance. Consider a team of autonomous aerial vehicles assigned to conduct a surveillance mission for purposes such as battle damage assessment related to required medical responses. Further, assume that one person is overseeing and controlling, when necessary, members of the team of aerial vehicles. In addition, assume that this mission is addressing the desire to collect information regarding where to send responders and how to most safely get them to those in need of help. As demonstrated in prior SERC research efforts (System Aware Cybersecurity), an adversary can, for example, execute an undetected cyberattack that hampers the ability to provide surveillance in selected areas that would be meaningful to our forces. Similarly, decoys or corrupted surveillance information could be used as means to misdirect our forces.

Experiments will include scenarios in which the user displays are augmented by *trust metrics* calculated on the basis of the consistency of sensor information. The relevant algorithms for trust metrics have already been developed in general form at UVA. Tuning the specifics of the experimental scenarios is anticipated to be a minor task. The trust metrics will serve to provide an augmentation of human intelligence for the task of assessing the trust-worthiness of the sensor information. This assessment task can be difficult for unaided humans if it involves assessing the correlations and consistency of networks of data sources, as is the case in many operational scenarios. The trust metrics are themselves the subject of operator confidence. Experiments will be conducted to understand the relationships between operator confidence in the metrics and their experience with them and with ultimate system outcomes. Results from the evaluations will be mapped into a first version of the desired methodology. In addition, based upon what is learned regarding the need for a broader set of experimental use cases, the needs for follow-on research will be illuminated.

Table 5.2-18 shows the focus, deliverables, and investment in the project through 2023.

Table 5.2-18. *Human Machine Team (HMT) Concepts for Resilient Autonomous Systems* Project Timeline

Year	Focus	Key Deliverables
Pre- 2018	Establish HMT performance concepts, metrics, and experimental protocols	Experimental protocols and outcomes
2019	In-depth analysis of experimental results	Advanced models of human roles in HMT
2020	Initiate development of reusable system test and evaluation processes that confirm that human performance has been appropriately been addressed	Engage with OT&E organizations to develop methodologies for employment of identified reusable processes
2021-23	To be determined	To be determined

The *Human Machine Team (HMT) Concepts for Resilient Autonomous Systems* transition plan and characterization are shown in Tables 5.2-19 and 5.2-20 below.

Table 5.2-19. *Human Machine Team (HMT) Concepts for Resilient Autonomous Systems* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	Review historical efforts related to resilience and human factors that were not necessarily focused on cyber attacks	• Plan Early
2	Establish a set of detailed experimental scenarios and protocols	• Plan Early • Pilot Continuously

#	Transition Action	Principles Implemented
3	Implement cyberattacks in simulation-in-the-loop (SITL) for an unmanned aerial system (UAS)	• Productize • Pilot Continuously
4	Conduct human-in-the-loop simulation (HITL) and analysis of the results	• Engage Community

Table 5.2-20. *Human Machine Team (HMT) Concepts for Resilient Autonomous Systems* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• Collaborating continuously with the Air Force Institute of Technology (AFIT) to examine the validity of experimental platforms, experimental protocols, and findings.
Progress (approval, adoption)	• None yet

5.2.5 TS Area Non-Core Funded Projects

During the time of the previous Technical Plan, the SERC has been awarded one TS non-Core funded projects. The project, which are briefly described in Table 5.2-21, is still active as of the time of the publication of this Plan.

Table 5.2-21. TS Area Non-Core Funded Project

Project	Sponsor	Description
Tools and methods framework for ship board power and energy systems	Naval Surface Warfare Center	This project is developing a method for comparing a set of power system architectures relative to a set of high-level capability requirements by capturing qualitative information from subject-matter experts (SMEs) in the decision framework to initiate a requirements decomposition process supporting a power system selection.
Security Engineering Decision Support Tool Trials	ARDEC	This project involved application of model-based engineering to a project addressing cybersecurity system requirements during the preliminary design phase for a hypothetical weapon system. The integrated application of three different model-based tools was investigated and results were very instrumental in informing design and development decisions regarding software implementation, cyber defense and cyber resilience. The model-based results proved to be persuasive regarding identification of user requirements, influencing system architecture derived by the systems engineering team and helping cybersecurity experts to make cost-effective trade-offs between software development processes, cyber defense solutions and cyber resilience solutions.

5.3 Systems Engineering and Systems Management Transformation (SEMT)

The research in SEMT over the past five years is creating an impactful change through increased understanding of the Digital Engineering landscape including strategic and tactical initiatives for a new operational paradigm between government and industry for Model-based Acquisition. These initiatives are needed in order to deliver capabilities to the warfighter at the speed of relevance in the face of continuous changing threats. These advances, however, create new research challenges, and we need to expand our thinking from individual systems to continuous tradespace analyses for mission, systems and subsystems in order to configure SoS to meet immediate threats, operational needs, lifecycle sustainment, workforce, model-based acquisition and the extended enterprises of both the government and industry. We live in a world where billions of sensors are connected to advanced computational capabilities and computational intelligence (e.g., AI, machine learning). These computational advancements not only live in the systems we deploy but must be leveraged in our new methods and practices that are enablers for Digital Engineering.

The cross-cutting aspects for SEMT are beginning to blend into the other focus areas of Enterprises and Systems of Systems to provide efficiencies that can be achieved by an Authoritative Source of Truth (AST) from an extended enterprise that includes both government and industry. The deployed systems and AST must be credible and trusted, The SEMT need for Human Capital Development requires more skills in applying MPTs enabled by modeling and computational intelligence. The dynamic needs for SEMT should apply the concept of Observe – to understand the environment, Orient – to align with what is important, Decide – to agree on the course of action, and Act to SEMT practices – the OODA loop. OODA is not only part of the operational systems SEMT seeks to develop, but also part of the needed SEMT practices. The OODA loop values agility over raw power and has been applied in business contexts as a way of gaining a competitive advantage. By being able to execute an OODA loop faster than a competitor (adversaries), it allows a company (the DoD) to stay ahead of the game, undermining a competitor's (adversaries) ability to respond. Finally, we must also recognize that the delivery of our research needs to keep pace with a computationally enabled world.

5.3.1 SEMT Vision and Current Progress

The SEMT Vision is to:

> *Develop methods, processes and tools to enable the transformation from sequential, document-driven, highly constrained practices toward much faster, flexible OODA-loop-supporting mission and enterprise-oriented approaches enabled by advances in modeling, simulation, data-driven analysis and artificial intelligence.*

These will enable much more rapid, flexible, scalable definition, development and deployment of increasingly complex future weapons systems.

The goal to achieve this vision is:

> *Prototype, demonstrate, and provide methods to continuously advance the transformation of systems engineering to dynamic processes that leverage the speed and rigor of rapidly evolving modeling, simulation and analysis computational technologies*

enabled by computational intelligence. Develop dynamic approaches for iterative procurement cycles that rapidly and concurrently develop cost-effective, flexible, agile systems to respond to evolving threats and mission needs.

The vision should factor in the Digital Engineering (DE) transformation goals as they were characterized by several organizations across DoD including OSD, Navy, Army and Air Force, and include:

- G1. Formalize the development, integration and use of models to inform enterprise and program decision making.
- G2. Provide an enduring authoritative source of truth.
- G3. Incorporate technological innovation to link digital models of the actual system with the physical system in the real world.
- G4. Establish a supporting infrastructure and environment to perform activities, collaborate and communicate across stakeholders.
- G5. Transform a culture and workforce that adopts and supports Digital Engineering across the lifecycle.

In keeping with its central position among the four SERC Research Areas in Figure 3-1, the SEMT research area includes collaborative efforts with the other three SERC research areas with respect to their Visions. This collaboration provides SEMT with greater understanding of how its research efforts can help address their Visions and provides SEMT with insights on how its research results can span multiple Visions.

An example of such collaboration is SEMT's research support of the ESOS Area Vision of creating SE principles and MPTs for SoS SE that generate affordable and overwhelming competitive advantage over current and future adversaries. SEMT's research results in cost estimation of SoS SE effort, combined with its results in SysML parametric architecture modeling and previous research efforts in the *Requirements for Net-Centric SE* Project conducted before the start of this Technical Plan, have been integrated to provide SoS SE cost estimation capabilities for affordable SoSs.

A further example involves SEMT's research support of the TS Area Vision of achieving much higher levels of system trust for the increasingly complex, dynamic, cyber-physical-human net-centric systems and systems of systems of the future. A workshop involving the TS *Systems Assurance* Project and the SEMT *Systems Qualities Tradespace and Affordability* Project has led to collaborative efforts in identifying and quantifying the synergies and conflicts among strategies for assuring security and safety qualities and strategies for achieving affordability, flexibility and mission assurance qualities.

Additional examples involve SEMT's research support of the HCD Area Vision of dramatically accelerating the professional development of highly capable systems engineers and technical leaders in DoD and the defense industrial base. Other examples include the previous SEMT *Graphical ConOps* Project research and the current *Interactive Model-Centric SE* Project, both focused on how to better support human visualization and decision support in defining and developing complex cyber-physical-human systems.

SEMT has combined insights from these collaborations and support of its OSD, Air Force, Army, Navy and DoD Agency research sponsors to formulate and create stronger SE and management foundations for addressing the SEMT Vision above. These foundations include set-based design of DoD systems, quantifying system qualities and system risks, an ontology for clarifying the complexities of system qualities and their interactions, and methods for evidence and risk-based decision support for evolutionary, concurrent SE and system development projects. All of these efforts continue to evolve and identify further challenges, as described in the plans below.

5.3.2 Strategies to Address the SEMT Vision

Digital Engineering is the foundation for the SEMT Vision as it is central to achieving a faster, flexible OODA-loop-supporting mission and enterprise-oriented approaches enabled by advances in modeling, simulation, data-driven analysis and artificial intelligence. The DE capabilities affect all dimensions of system engineering and the system life-cycle. The potential and impact of DE cannot be overestimated. However, there are additional areas of research focus that are essential to realizing the full potential of DE.

One of the key areas is Artificial Intelligence (or Augmented Intelligence) (AI) and Machine Learning (ML). While many of these advances are being driven by commercial companies in search, social media and autonomous transportation, systems engineering will need to bring these capabilities into its DE toolkit. The SERC should leverage these types of capabilities in the systems we deploy, but also in the tools, methods and computationally enabled environment we use to conceive, analyze, develop and verify and validate ever more complex, adaptive and autonomous systems that are part of a broader system of systems providing evolving capabilities that are needed for evolving threats.

Knowledge representation plays a key role in applying Artificial Intelligence, and ontologies are a critical means for representing knowledge that are necessary to support domain specific model federations. Ontological efforts have shown success in helping understand the human genome, but there has been less use so far for systems engineering. There is ongoing work in ontologies and some organizations such as NASA/JPL are beginning to share their efforts mostly to develop and use the ontologies. In addition, ontologies and semantic technologies have also been shown to assist in enforcing methods, and the formalization of knowledge in ontologies is an enabler for reasoning about methods. Interoperable ontologies should allow us to reason about systems engineering across domains.

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. Thus, validation-continuous processes and capabilities become more important. Digital Engineering formalizes the representation of alternative analysis, CONOPs (e.g., using gaming), mission, systems, and early and as-built design into a “software” problem, and therefore this enables continuous validation (and verification) in a new way throughout the lifecyle. One catalyst is providing capabilities to the warfighter more quickly and being able to continuously adapt to changing threats in half the time of traditional systems of large-scale systems. Every existing process and procedure should be understood to see how it can be supported and accelerated by DE.

Finally, system emphasis in all domains is moving rapidly from capabilities to mission success. This has been the trend for some time in the commercial world and is now being realized as being critical in defense systems. The ability to rapidly compose and validate mission capabilities is critical. One of the cornerstones for this is Digital Engineering Collaboration through Authoritative Source of Truth (AST). There are many opportunities to increase the speed of interactions between Government and Industry contractors through a Collaboration through AST. The NAVAIR surrogate pilot is demonstrating a number of use cases. We have shown how our concept can address data rights and intellectual property issues, but there are many other challenges not being addressed by the research, such as security.

Successfully executing the following strategies will make significant progress towards addressing the SEMT Vision:

1. *Blaze the Trail to Digital Engineering:* Explore the practical and effective application of Model-Based Systems Engineering to lead to more coherent, rapid and responsive system acquisition and development. Develop MPTs for Digital Engineering based on practical work within DoD engineering and acquisition. Key challenges are: model trust, model curation and uncertainty quantification.
2. *Bring the Power of AI to DoD Systems:* Develop systems engineering strategies for requirements analysis, verification and validation of autonomous systems, supported by automated methods and tools. Also develop system design and decision support tools that exploit the power of machine learning for rapid and effective mission engineering and systems engineering.
3. *Balance Velocity, Risk and Performance:* Develop system design and acquisition MPTs that quantify the benefits and costs of rapid deployment, technical and program risk, and system performance to dramatically accelerate the delivery of technology-enabled capabilities to the warfighter.

Compose Capabilities for Mission Impact: Develop a rigorous strategy for effective and rapid Mission Engineering and support the strategy with MPTs for mission design and mission decision-making.
Three current Core-funded SERC research programs have been implementing these strategies:

- Digital Engineering (formerly Interactive Model-Centric Systems Engineering)
- SE Methods for AI and Autonomous Systems (New)
- Systems Engineering for Velocity and Agility (formerly: Affordability and Value in Systems, Quantitative Risk, & Agile Systems Engineering)

In addition, SEMT has been successful in attracting complementary funding from the Air Force Space and Missile Command, the Army Engineer Research and Development Center, several Navy organizations, the Marine Corps, and the National Science Foundation, all of which extend and experimentally apply the capabilities developed under Core funding.

5.3.3 Digital Engineering Program

The SERC has been successful over the past seven years researching and developing methods, processes and tools to support digital engineering, particularly in programs such as the Systems Engineering Transformation Surrogate Pilot and Interactive Model-Centric Engineering. Meanwhile, Digital Engineering is permeating the DoD and becoming the clear technological basis for developing future systems. The next phase of Digital Engineering research will focus on filling the gaps in current digital engineering technology, with projects on model integrity and model composability, exploring the interaction between engineers and modeling tools with projects exploring the allocation of tasks between humans and computers, and integrating model-centric digital engineering into the acquisition project.

Projects in Model Integrity will develop methods for measuring the quality of the outputs from design models, methods for model verification and validation, and methods for certifying and managing the configuration of models that serve as the authoritative source of truth in a digital engineering environment. These projects will draw on recent work in uncertainty quantification and model verification and break new ground in the configuration management of engineering models. In addition, research in curation and configuration management will lead to the development of appropriate tools and techniques.

Projects in Model Composability will address the most critical challenge in current engineering development environments: the integration of disparate design, performance and quality models together to create a complete description of the system being designed. Most of the models used by engineers do not communicate well with each other due to imprecise definitions of variables, differing levels of granularity, differing time bases for simulations, and many other issues. Projects in Model Composability will develop practical solutions to these barriers to comprehensive digital engineering.

Projects in Human-Computer Task Allocation will address balancing the digital engineering toolset to best exploit the unique talents of skilled engineers and the power of models and data bases that support engineering.

Finally, and perhaps most importantly, projects in Model-Centric Acquisition will bring the advantages and power of digital engineering to the contracting and contract management processes that are at the heart of system acquisition. These projects will develop prototype contracts that replace natural language requirements with digital models and pilot the integration of contractor and government models within the digital engineering environment.

The objectives of the research are cross-cutting and interrelated, as shown in Figure 5.3-1. The research needs to expand on the prior research and include specific focus on technological aspects to address the research gaps in the context of the SET Framework, but still include cross-domain model integration, model integrity, ontologies, semantic web technologies, modeling methods, multi-physics modeling, and model visualization.

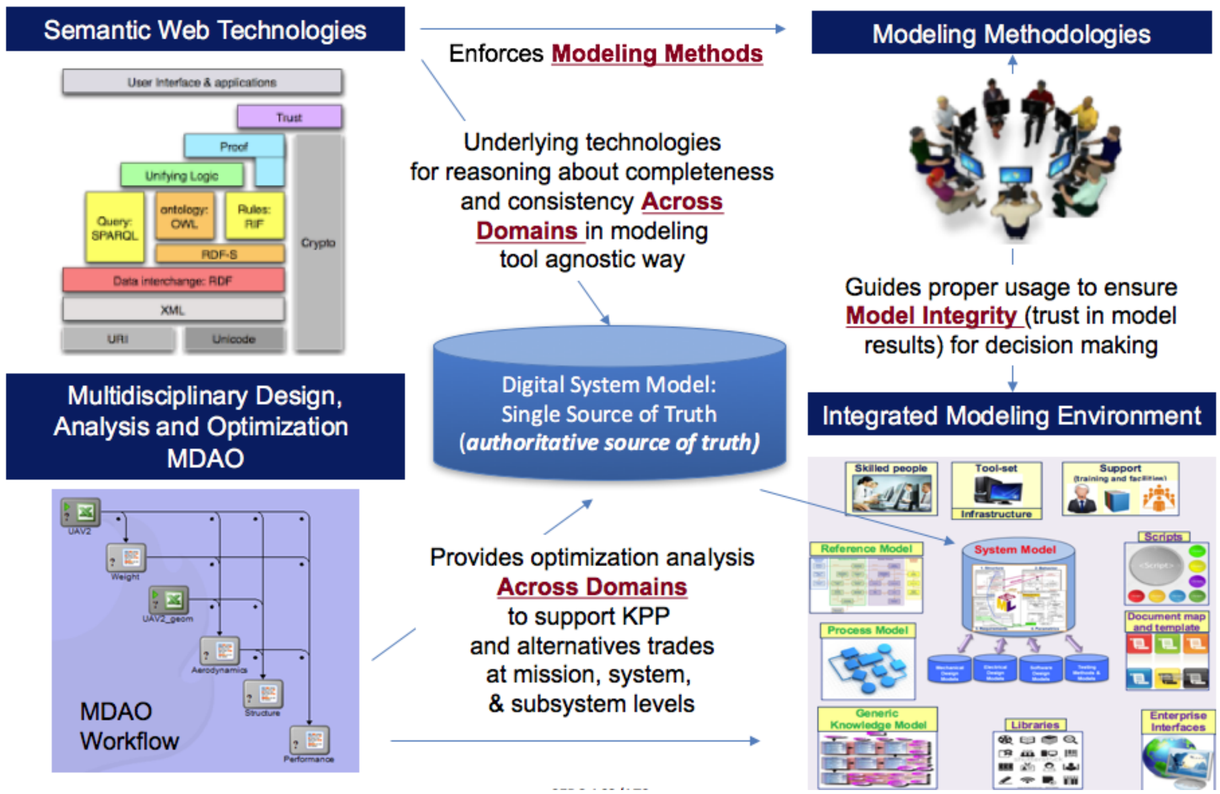

Figure 5.3-1. Cross-cutting Relationships of Research Needs (Source: Transforming Systems Engineering through Model-Centric Engineering, SERC-2018-TR-103, February 28, 2018)

This research program, which currently has one Core-funded project, primarily implements all four of the SEMT strategies, and numerous non-Core funded projects, in particular *Transforming Systems Engineering through Model-Centric Engineering*. Table 5.3-1 summarizes the active projects and the strategies it primarily supports.

Table 5.3-1. Projects in the Digital Engineering Program

Projects	Started	Purpose	Primary SEMT Supported Strategies
Interactive Model-Centric Systems Engineering	Late 2013	Use models to drive systems engineering, development, production, and evolution	1, 2, 3, 4
Transforming System Engineering	Late 2013-2014	Global scan of Industry, Government and Academia to understand the state-of the-art of a holistic approach to MBSE/MCE	1, 2, 3, 4

through Model-Based Systems Engineering		Develop a common lexicon for MBSE, including model types, levels, uses, representation, visualizations, etc. Model the "Vision," but also relate it to the "As Is" process Integrate a Risk Management framework with the Vision	
Transforming System Engineering through Model-Centric Engineering (MCE)	2015	Communicate and report out on the state of Model Centric Engineering that are evolving at an accelerating pace of over 30 organizations Produce 700 element Lexicon on "everything" related to "model" Characterize canonical elements of an Integrated Modeling Environment gleaned from global survey and characterize the gaps that must be filled to realize the Vision Characterize the facets and elements of an Integrated Framework for Risk Identification and Management	1, 2, 3, 4
Transforming Systems Engineering through MCE	2016	Research challenges identified by prior research to realize vision: Model Cross-Domain Integration Cross-domain integration of models to address the heterogeneity of the various tools and environments that will leverage High Performance Computing Model integrity to ensure trust in the model predictions by understanding and quantifying margins and uncertainty Modeling methodologies that can embed demonstrated best practices and provide computational technologies for real-time training within digital engineering environments Research Multidisciplinary Design Analysis and Optimization (MDAO) applied to mission models and system models	1, 2, 3, 4
Transforming Systems Engineering through MCE	2017	Characterize how the MCE research aligns with concept of the NAVAIR Systems Engineering Transformation (SET) Framework for a new operational paradigm between Government and Industry Define the objectives and use cases for assessing and refining the SET Framework using SET Surrogate Pilot Research Multidisciplinary Design Analysis and Optimization (MDAO) applied to Graphical Concept of Operations (CONOPS) Develop a formalization	1, 2, 3, 4
Transforming Systems Engineering through MCE	2018	Establish an MCE environment for a Collaborative Authoritative Source of Truth for performing experiment through the SET Surrogate Pilot Develop the SET Surrogate Pilot Plan, Mission, System, Statement of Work, and Request for Proposals completely in models to perform experiment with model-based acquisition and source selection using a Surrogate Contractor Develop an Interoperability and Integration Framework that demonstrates a Decision Framework through integration of MDAO, SysML, OpenMBEE, semantic web technologies, a decision ontology, and visualization of alternative analysis tradeoffs, including Key Performance Parameters	1, 2, 3, 4

5.3.3.1 Interactive Model-Centric Systems Engineering Project

Models have significantly changed SE practice over the past decade. Most notably, model-based systems engineering (MBSE) methods and tools are increasingly used throughout the entire system lifecycle to generate systems, software and hardware products, and replacing labor-intensive and error-prone documentation-based processes with model-based ones. While substantial benefits have been achieved, the most impactful application of models in SE has yet to be realized. Truly transformative results will only come through intense human-model interaction, to rapidly conceive of systems and interact with models in order to make rapid trades to decide on what is most effective given present knowledge and future uncertainties, as well as what is practical given resources and constraints. The *IMCSE* Project seeks to enable this transformation.

The IMCSE research program arises from the opportunity to investigate the various aspects of humans interacting with models and model-generated data. This is an important problem because human effectiveness in performing digital model-based engineering and human acceptance of model-centric practice will be essential components of success of future acquisition programs. This is a multi-faceted investigation that involves both technical and social facets. Evidence-based findings are not readily found; but this is necessary to avoid failures grounded in using incorrect assumptions and ignoring cognitive and perceptual limitations. Open areas of inquiry include: how individuals interact with models; how multiple stakeholders interact using models and model generated information; facets of human interaction with visualizations and large data sets; how trust in models is attained; and what human roles are needed for model-centric enterprises of the future. This project is based on a belief that improving human-model interaction and social dimensions of model-based environments will significantly improve the effectiveness of digital model-based engineering practice, quality of model-decision making, and cultural acceptance of a digital future.

The SERC performed IMCSE research in Phases 1 through Phase 5 focused in six areas:

1. **Pathfinder Project and Research Roadmap.** This project investigated the current state of interactive model-centric systems engineering, producing a report that identified many research opportunities, gaps and issues. The pathfinder project continued to elicit information on the state of the IMCSE art and practice, through a workshop and additional meetings with stakeholders and potential research partners. A research roadmap was defined, and several topic areas were explored in more depth with findings documented in technical papers.

2. **Interactive Schedule Reduction Model (ISRM**). This effort built on an existing prototype model to study alternatives for interactively exploring reduction of development schedule and application of resources. An open-source interactive demonstration prototype was completed and made available.

3. **Interactive Epoch-Era Analysis (IEEA).** This activity initiated an effort to extend a current approach for evaluating systems under uncertainty, epoch-era analysis (EEA) through interactive capability, resulting in a findings report, initial application, and plans for further development and case studies. The approach for evaluating systems under dynamic uncertainty using epoch-era analysis was evolved, with focus on enhanced interactive capability and allowing for scaling for big data analysis. The framework and supporting tools were used to complete a defense-oriented demonstration case and demonstration prototypes were developed for single epoch analysis and multi-epoch analysis and made available. Research extended the IEEA framework and developed updated prototypes, which were applied on an on-orbit servicing vehicle case as an impact assessment of pilot (proxy) application with a university research partner. An experiment to investigate the impacts of visualization and interaction in a decoupled manner was initiated. The IEEA framework and prototypes were applied in a commercial ship design case to test applicability

to a non-defense application and analysis of changeability options. The designed experiment on impacts of decoupled visualization and interaction was completed. The framework, prototypes, case-based impact studies, and experiment results were completed.

4. **Model Tradeoff and Choice.** A framework for conducting value model trades and evaluative (performance, cost) model trades was developed and tested to validate the framework and identify workflow considerations. A demonstration case for interactive model-trading, including value, performance, and cost models with inherited data was completed to demonstrate impact on system decision making.

5. **Cognitive and Perceptual Considerations in Human-Model Interaction.** An investigation was initiated to better understand cognitive and perceptual considerations in human-model interaction. An analogy case on the transition from traditional to glass cockpits was performed to gather empirical knowledge on challenges and preliminary strategies for using complex interactive model-centric environments. Empirical investigation of the needs and desires for the interactive experience from the perspective of users of model-centric environments continued. Research was completed on a study on framing multi-stakeholder tradespace exploration. An interview-based study on model-centric decision making and trust was designed and initiated. The empirical study on model-centric decision making was completed with thirty experts, resulting in findings and preliminary guiding heuristics. Outcomes of the investigation of human-model interaction were compiled into an integrated state of the practice white paper. A technical exchange workshop was held to gather practitioner feedback on study results and directions for transitioning heuristics to practice.

6. **Curation of Model-Centric Environments.** The needs and benefits of formal curation of model-centric environments was investigated through stakeholder discussions. Initial research investigated the potential role/responsibilities for a curation function in interactive model-centric environments. Researchers investigated alternative forms for curation leadership, curation practices, and data/model pedigree, and evolved a concept for an assessment instrument for curation capabilities. A technical exchange session was held to gather feedback on interim research and identify transition partners. As this is an area of great importance to the DoD community, a new Research Topic is being created at the time this Plan was published.

Phase 6 research provides the opportunity to mature and extend the research outcomes of prior phases, and further transform findings into specific MPTs for enhancing effectiveness of model-centric enterprises. Evidence-based strategies, guiding principles, and assessment frameworks will contribute to effectiveness of programs and enterprises, and transformation to digital model-based engineering. Prior phase research has generated expert-based interview findings and heuristics for human-model interaction and decision-making. In this phase of the research an iterative evaluation, aggregation and selection approach will be used to converge on consensus-based heuristics. Pilot application and supporting secondary data will be employed to test and finalize the set of guiding principles to support informed decision making. Each principle will be fully described, including one or more application examples. Two pilot applications using the principles and supporting information will be developed and evaluated, including a teaching module for use in an undergraduate engineering leadership program and a segment for use in a model-based engineering program team launch. Possible approaches for using patterns and pattern languages for capturing human-model interaction will be investigated.

Prior phase research has identified sociotechnical leadership capabilities that provide the ability to execute digital model-based engineering at the program and enterprise levels. A framework for assessing model-centric enterprise capabilities will be developed using an evidence-based approach, which integrates empirical research evidence, decision maker/practitioner's expertise, and situational perspectives (values, needs, stakeholder preferences such as risk tolerance). The assessment framework will accommodate assessing capability respective to the state of transformation from traditional to fully digital model-based engineering. Model-centric enterprise capabilities identified in prior phase research include model composability, transparency, accession practices, model valuation practices, model trust and others. Ultimately, having a common framework for model-centric enterprise capabilities enables better understanding of effective practices, accessing transformation progress and generation of evidence through systematic study, providing benefits across the systems community.

Table 5.3-2 shows the focus, deliverables and investment in the IMCSE Project through 2023 aimed at addressing the three tasks above, as well as new tasks in out-years.

Table 5.3-2. *IMCSE* Project Timeline

Year	Focus	Key Deliverables
Pre-2018	Investigated and demonstrated enhanced human-model interactivity of existing methods and practice. Generated foundational knowledge in several human-model interaction related areas	MPTs, Demonstration Prototypes, Application Case Studies, publications
2019	Evolved and expanded guiding principles for human-model interaction and establish a framework for assessing model-centric enterprise capabilities, with a focus on model curation leadership	Guiding practices, knowledge artifacts, capabilities framework, principles and lexicon transitioned into standards and community-generated products, publications
2020	Evolved and expanded set of formal patterns for human-model interaction. Pilot use of guiding principles in model-centric enterprise practices	Enablers and case application, human-model interaction patterns, application demonstrations, publications
2021-23	Investigate and develop strategies for using human-model interaction patterns to enable augmented intelligence in systems and enterprise model-based environments. Expand human-model interaction patterns to digital twins of operational systems	Demonstration cases and prototypes, publications

The *IMCSE* transition action plan and characterization are shown in Tables 5.3-3 and 5.3-4 below.

Table 5.3-3 *IMCSE* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	The *IMCSE* Project has been developed using three complimentary thrusts (foundations, fundamentals, applications) with different timescales, to have impact on the long term, near term and the present. An over-arching project goal is to build a community of interest around IMCSE.	• Plan Early • Balance Long and Short Term • Engage Community

#	Transition Action	Principles Implemented
2	An *IMCSE* Pathfinder Workshop engaged members of the community in characterizing state of the art/practice, identifying research needs, and envisioning the model-centric environment of the future. A workshop report was published and distributed. Efforts to gather research needs and develop broader collaboration on longer term research agenda have been initiated.	• Engage Community • Balance Long and Short Term
3	A proof-of-concept prototype for the Interactive Schedule Reduction Model was completed, demonstrated to practitioners, and software made available through a website.	• Engage Community • Pilot Continuously • Productize
4	A pre-existing method (Epoch-Era Analysis) has been adapted for higher level of interactivity, with case demonstrations and application cases. The resulting body of work is available as an example for transforming traditional methods to interactive methods.	• Engage Community • Pilot Continuously • Productize
5	Prototype visualization tools for Interactive Epoch-Era Analysis have been piloted with research stakeholders and demonstrated to practitioners. Several interactive demonstration prototypes are available online to gain feedback, with continuing updates planned as the MPT matures. Findings on visual interaction from two experiments have been published and presented.	• Engage Community • Pilot Continuously • Productize
6	Guiding principles have been generated based on several investigations, including an interview-based study with 30 model experts. Heuristics and resulting principles have been presented to the stakeholder community in numerous events and conferences. Pilot use in transformation programs and education is ongoing. Validated principles will be published in the SEBOK.	• Engage Community • Pilot Continuously • Productize
7	Model curation capabilities, leadership role and responsibilities have been defined and the stakeholder community has been engaged in various ways to further the work. The research has been presented to government, industry and academic audiences in invited talks, meetings and conferences	• Engage Community • Pilot Continuously • Productize
8	Model trade-off case studies for value models, performance and cost models have been completed and made available.	• Productize • Pilot Continuously
9	*IMCSE* has held knowledge exchanges, collaborated with, and discussed future pilot opportunities with several other universities, FFRDCs and non-profits, and government agencies, and has given numerous invited talks at key events.	• Productize • Engage Community

Table 5.3-4. *IMCSE* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• *IMCSE* Technical Reports and the *IMCSE* Pathfinder Workshop Report are available to the SERC community. Several demonstration prototypes with documentation can be accessed freely and downloaded. An *IMCSE* paper at 2016 CSER paper received the MITRE Best Systems Engineering Research Transition Award.

Characteristic	Evidence
Progress (approval, adoption)	• *IMCSE* has effort has resulted in 5 SERC technical reports, 1 journal paper, 12 published referred conference papers, 15 conference presentations, 6 invited talks, 3 webinars, one pathfinder workshop (report published), and numerous technical exchange meetings • *IMCSE* SERC Talk is the most highly viewed webinar in the SERC series • *IMCSE* research was presented as invited talks in model-based transformation summits at JPL (2016) and The Aerospace Corporation (2018) • Selected research findings are shared in the MIT online certificate program, Architecture and Systems Engineering: Models and Methods to Manage Complex Systems, hosted on the Ed-X platform, in partnership with NASA and Boeing • An *IMCSE* paper received the 2014 SERC Best Student Paper Award and another IMCSE paper received the CSER 2015 Best Academic Paper Award. An IMCSE paper at 2016 CSER paper received the MITRE Best Systems Engineering Research Transition Award. • Model curation lexicon is being adopted by the Digital Engineering Information Exchange Working Group.

5.3.3.2 Transforming Systems Engineering through Model-Centric Engineering

Model-centric engineering is a digital engineering approach that integrates different model types with simulations, surrogates, systems and components at different levels of abstraction and fidelity across disciplines throughout the lifecycle. Industry is trending towards higher integration of computational capabilities, models, software, hardware, platforms, and humans-in-the-loop. The integrated perspectives provide cross-domain views for rapid system level analysis allowing engineers from various disciplines using dynamic models and surrogates to support continuous tradespace decisions in the face of changing mission needs.

While modeling everything may not be practical for all projects, the plan is to use models to the extent possible in order to demonstrate the feasibility and desired methods that will be captured as examples in reference models. The pilot is developing an experimental Unmanned Aerial Vehicle (UAV) system called Skyzer. The focus is on learning about a new operational paradigm between government and industry in the execution the SET Framework, not necessarily to produce an entire air vehicle design. There are many more detailed facets to the surrogate pilot that are discussed in this report, and the surrogate pilot, which had an official kickoff in December of 2017, is ongoing through 2018.

Another objective under consideration in the context of the operational model is to replace large-scale document-centric reviews such as Systems Requirements Review (SRR), System Functional Review (SFR), Preliminary Design Review (PDR), etc. with continual event-driven reviews using objective evaluation based on model-centric information. NAVAIR needs an objective decision framework to assess evolving design maturity with considerations of value to the KPPs, risk and uncertainty. This is another objective for the surrogate pilot.

The strategic plans of SET and overarching goals of this research have been expanded through *Transforming Systems Engineering through Model-Centric Engineering Phase 4.* This research has collaborators from Stevens Institute of Technology, Georgia Institute of Technology and University of Maryland, in addition to the surrogate pilot team that includes a Surrogate Contractor, and team members from NAVAIR and NAVAIR contractors. We are also working collaboratively with US Army RDECOM-ARDEC in Picatinny, NJ and some of the research results derived from those efforts that are being leveraged in the surrogate pilot are discussed in this report. We are also leveraging research efforts from *Verification* *and Validation (V&V) of System Behavior Specifications* and the Naval Postgraduate School Collaborators. Additional research associated with this research is planned for *Transforming Systems Engineering through Model-Centric Engineering Phase 5*.

ARDEC research has created awareness about research challenges, opportunities and emerging trends overlap with some of the challenges areas described by NAVAIR, but with more focus on technologies models, software, and prototypes that contribute to the vision for the modeling and infrastructure for the AVCE integrated Model Based Engineering (iMBE) environment, such as modeling methods and technologies for interoperability and integration of mission, system, and multi-domain models, semantic web technologies, Multidisciplinary Design, Analysis and Optimization (MDAO), and graphical concept engineering (CONOPS) using gaming technologies. These technologies are often new, and the research also documents methods and lessons learned. Aligning with the leading-edge work from National Aeronautics and Space Administration (NASA) Jet Propulsion Laboratory (JPL) the team developed several Docker configurations for deployment of OpenMBEE that enables the use of the Model Development Kit/DocGen, the Model Management System (MMS) and View Editor. This instantiation of OpenMBEE has been integrated into our Interoperability and Integration Framework (IoIF) for our use case to integrate SysML models with the ARDEC inspired Decision Framework, a decision ontology based on the Basic Formal Ontology using semantic web technology, with output visualizations using Tableau. Those research thrusts were characterized as sixteen MBSE use cases to demonstrate and evolve IoIF to research technological aspects that include cross-domain model integration, model integrity, ontologies, semantic web technologies, modeling methods, decision analysis framework, MDAO, multi-physics modeling, model visualization and integrated modeling environments supporting an authoritative source of truth (AST) that can contribute to ARDEC's AVCE iMBE vision. All of the decisions that have been made during this project have been collected on an open collaboration site which should facilitate the broad transition of this work.

Table 5.3-5 shows the focus, deliverables and investment in the Transforming Systems Engineering through Model-Centric Engineering Project through 2023.

Table 5.3-5. *Transforming Systems Engineering through Model-Centric Engineering* Project Timeline

Year	Focus	Key Deliverables
Pre-2018	Systems Engineering Transformation (SET) Research on cross-domain model integration, MDAO and Objectives for SET Surrogate Experiments Characterization of capabilities, constraints for an integrated modeling environment to support Model Centric Engineering	Integration of research using SE Transformation Surrogate Experiments and demonstration of collaboration in Authoritative Source of Truth Demonstration of the benefits of semantic web technologies for interoperability with prototypes, models, and knowledge transfer through deep-dive working sessions
2019	Increment 2 with additional SET Surrogate experiments for other objectives such as model management, Capability-Based Test and Evaluation, Airworthiness and visualization Extensions of Interoperability and Integration Framework to integrate other ARDEC domains with decision ontology hierarchical relating mission and system capabilities	Capture reference models derived from Increment 1 of Surrogate experiments and associated characterization of model methods and model management methods Interoperability and Integration Framework that provides demonstrations of linking integrated modeling environment with mission and system models, with semantic web technologies

Year	Focus	Key Deliverables
2020	Increment 3 with additional SET Surrogate experiments to bring in additional disciplines across other life cycle phases and competencies such as Logistics, Dependability, Mission Systems and cyber	Capture reference models derived from Increment 2 of Surrogate experiments and associated characterization of model methods and other methods cutting across life cycle and disciplines Demonstration of approaches needed for model integrity (trust in models and simulation)
2021-23	The use Artificial Intelligence, Augmented Intelligence and Machine Learning to automating the systems engineering practices supported by underlying knowledge representation of ontologies	Demonstration of the capabilities driven by leveraging the SET Surrogate Pilot models.

The *Transforming Systems Engineering through Model-Centric Engineering* transition action plan and characterization are shown in Tables 5.3-6 and 5.3-7 below.

Table 5.3-6. *Transforming Systems Engineering through Model-Centric Engineering* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	The TSE4MCE Project focused early on understanding the most advance and holistic approaches to MCE, and providing and understanding of this global scan to senior executives at NAVAIR and DoD, delivering traceable evidence of many advanced uses of MCE, a 700-element lexicon, a vision for the future state and two challenges areas: cross-domain and multi-physics model integration, and establish and quantify model integrity, both which should be enabled by evolving High Performance Computing	• Plan Early • Balance Long and Short Term • Engage Community
2	The TSE4MCE global scan help senior executives at NAVAIR more deeply dig into the art-of-the-possible for MCE in order to radically change the current operational paradigm, and industry embrace the challenge to work in new ways enable by rapidly accelerating MCE technologies and methods	• Plan Early • Balance Long and Short Term • Engage Community
3	Senior leadership at NAVAIR understands that they must move quickly to keep pace with other organizations that have adopted MCE and must transform in order to perform effective oversight of primes that are using modern modeling methods for system development. This resulted in aligning the research gaps and challenges for a Systems Engineering Transformation (SET) Framework – a new concept for a paradigm change for acquisition that maps to the Digital Engineering Strategy	• Plan Early • Balance Long and Short Term • Engage Community • Pilot Continuously
4	Broad roll out of functional areas at NAVAIR, including Research on Model Integration, Model Integrity, Ontology, MDAO, Multi-Physics Modeling, Model Visualization, Roadmap & Implementation conducted in the context of a SET Surrogate Pilot using collaborative Authoritative Source of Truth. Demonstrable capabilities levering and support community such as OpenMBEE that is deployed for both NAVAIR and ARDEC to demonstrate art-of-the-possible	• Plan Early • Balance Long and Short Term • Engage Community • Pilot Continuously • Support Centrally • Productize

Table 5.3-7. *Transforming Systems Engineering through Model-Centric Engineering* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• TSE4MCE Technical Reports are available to SERC community. The results convinced NAVAIR leadership that resulted in the NAVAIR SE Transformation. These reports demonstrate relevance, because they have been referenced by Industry Collaboration such as the Aerospace Industry Association and National Defense Industrial Association.
Progress (approval, adoption)	• SERC Research is one functional area of the broader SET Functional Areas that include: Workforce & Culture, Integrated Modeling Environment, Process and Methods, Policy Contracts and Legal, and SET Enterprise Deployment (which own the SET Surrogate Pilot Experiments) • Conducting experiments in the context of the SET Surrogate Pilot involving teams for mission, system, statement of work, request for proposal, and source selection all performed in terms of models. The effort, results, models, lessons learned are publicly available through the All Partners Network and using the OpenMBEE environment on an Amazon Web Service server. • Involving industry as part of the Acquisition System Reference Model. • 77 SERC Technical Reports • 1 Journal paper in the Journal of Defense Modeling and Simulation, 2017 with Sponsors as Co-authors • 10 papers in Proceeding in conferences such as CSER, INCOSE, IEEE Systems Engineering, Complex Adaptive Systems • 15 presentations at NDIA SE Conference, OpenMBEE Collaborator Group, System of Systems Engineering Collaborators Information Exchange, and SERC events • Industry and Government Forum for Model Centric Engineering • Collaborations with Aerospace Industry Association, Semantic Technologies for Systems Engineering, OpenMBEE, Open Collaboration Group for MBSE, Digital Engineering Working Group, National Defense Industrial Association Modeling and Simulation Group

5.3.4 SE Methods for AI and Autonomous Systems Program

Autonomous systems, and particularly systems controlled through artificial intelligence technology, have limited and constrained potential when developed under conventional natural language requirements, such as “shall” statements. The power of these systems is often in their ability to improvise or learn effective behaviors in unforeseen circumstances but improvised and learned behaviors cannot be specified at the start – instead they are created after the system is developed.

Initial projects in this area will create a new way of specifying requirements for autonomous and intelligent systems, and construct and test prototype toolsets to implement the new methods. Initial efforts will build on use case techniques that have been successful in commercial software developments and adapt these methods to the DoD requirements management processes. Further projects will research methods of verification testing of requirements that utilize new methods of specification. These projects will explore incorporation of requirements and verification tests into system development contracts with industry.

Additionally, this area will explore new approaches to system validation, creating more definitive processes that implement validation throughout the lifecycle, from pre-milestone A activities through initial operating capability. A stronger, more coherent approach to validation will compensate for the loosening of detailed behavioral specifications that will be necessary to gain the full benefit of learning, autonomous weapon systems.

Table 5.3-8 summarizes the active projects and the strategies they primarily support.

Table 5.3-8. Projects in the *SE Methods for AI and Autonomous Systems* Program

Projects	Started	Purpose	Primary SEMT Supported Strategies
Next generation Adaptive Cyber-Physical Human Systems	September 2017	Develop Conceptual framework and testbed to model and prototype adaptive cyber-physical-human systems	System Assurance; Trusted Resilience
Formal Methods in Resilient Systems Design using a Flexible Contract Approach	August 2016	Develop Formal Methods for Resilient System Design using a flexible contract approach.	System Assurance; Trusted Resilience

5.3.4.1 Next generation Adaptive Cyber-Physical Human Systems

Cyber-Physical-Human (CPH) Systems are purposeful arrangements of sensors, computers, communication devices, and humans to perform tasks that achieve specific mission objectives. These systems typically allow other systems, devices, and data streams to connect/disconnect as needed during mission execution. The roles of humans in CPH systems are quite varied. In adaptive CPH systems, humans collaborate with the cyber-physical elements to jointly accomplish tasks and adapt to changing contexts to accomplish mission goals. Mutual adaptation based on prior knowledge, cognitive modeling, and online machine learning are key characteristics of adaptive CPH systems. This project is focused on developing a conceptual framework and testbed to model and prototype adaptive cyber-physical-human systems.

Table 5.3-9 shows the focus, deliverables and investment in the Next generation Adaptive Cyber-Physical Human Systems Project through 2023.

Table 5.3-9. *Next generation Adaptive Cyber-Physical Human Systems* Project Timeline

Year	Focus	Key Deliverables
Pre-2018	Defining CPHS, ontology, and problem formulation	2018 INCOSE IS Paper, End-of-Year 1 technical report
2019	Finalize Ontology, Create Transition Plan, Explore Machine Learning, Develop Dashboard	End-of-Year technical report, working dashboard prototype
2020	Expand data collection and incorporate machine learning capability	End-of-year report

Year	Focus	Key Deliverables
2021-23	To be determined based on follow-on funding	To be determined

The *Next generation Adaptive Cyber-Physical Human Systems* transition action plan and characterization are shown in Tables 5.3-10 and 5.3-11 below.

Table 5.3-10. *Next generation Adaptive Cyber-Physical Human Systems* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	Build Prototype Dashboard	• Early prototyping to engage community
2	Integrate dashboard with simultaneously operating simulated and physical systems with facilities for monitoring and visualization	• Early proof of feasibility to minimize integration risks
3	Test Cyber-Physical system behavior by flying physical hardware platform with live monitoring of platform flight	• Hardware-in-the-loop feasibility demo – key building block for adaptive CPHS

Table 5.3-11. *Next generation Adaptive Cyber-Physical Human Systems* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• Demonstration of Successful flight and vehicle control through dashboard served to establish feasibility and practicality of overall system concept; demonstrated capability in the Pentagon to SERC sponsor; published accomplishments in INCOSE 2018 International Symposium, 2018 Systems Conference (NDIA), and submitted paper to MDPI Open Source Systems Journal
Progress (approval, adoption)	• Successfully replaced simulated model with actual hardware using the same interface – a key advance in demonstrating capability of CPHS testbed; published paper describing capability in above three venues; demonstrated capability in the Pentagon to SERC sponsor

5.3.4.2 Formal Methods in Resilient Systems Design using a Flexible Contract Approach

Resilience is a much-needed characteristic in systems that are expected to operate in uncertain, disruptive environments for extended periods. Resilience approaches today employ ad hoc methods and piece-meal solutions that are difficult to verify and test, and do not scale. Furthermore, it is difficult to assess the long-term impact of such ad hoc "resilience solutions." This research presents a flexible contract-based approach that employs a combination of formal methods for verification and testing, and flexible assertions and probabilistic modeling to handle uncertainty during mission execution. A flexible contract (FC) is a hybrid modeling construct that facilitates system verification and testing while offering the requisite flexibility to cope with nondeterminism. This research illustrates the use of FCs for multi-UAV swarm control in partially observable, dynamic environments. However, the approach is sufficiently general for use in other domains such as self-driving vehicle and adaptive power/energy grids

Table 5.3-12 shows the focus, deliverables and investment in the Formal Methods in Resilient Systems Design using a Flexible Contract Approach Project through 2023.

Table 5.3-12. *Formal Methods in Resilient Systems Design using a Flexible Contract Approach* Project Timeline

Year	Focus	Key Deliverables
Pre-2018	Developing Dynamics and Probabilistic Decision-Making models, Assembling Quadcopters,	2 Final Technical Reports, 2 conference papers
2019	Transferring Probabilistic Decision-Making Algorithms on Hardware, refining previous models, creating transition plans	Final Technical Report
2020	Perform Data Collection and refining models	Final Technical Report
2021-23	To be determined based on follow-on funding	To be determined

The *Formal Methods in Resilient Systems Design using a Flexible Contract Approach* transition action plan and characterization are shown in Tables 5.3-13 and 5.3-14 below.

Table 5.3-13. *Formal Methods in Resilient Systems Design using a Flexible Contract Approach* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	Prototype quadcopters	• Reduced Scale Model with requisite physical characteristics
2	Demonstrate system modeling approach and capability to switch between system model simulation and Hardware-in-the-loop simulation	• Engage community through early demonstration of core concepts
3	Demonstrate common interface to simulated quadcopter model and physical quadcopter	• Common interface conveys seamless substitution of simulation with actual hardware

Table 5.3-14. *Formal Methods in Resilient Systems Design using a Flexible Contract Approach* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• Demonstrated successful flight with off-the-shelf components thereby showing practicality of the prototype; demonstrated capability in the Pentagon to SERC sponsor; published accomplishments in INCOSE 2018 International Symposium, 2018 Systems Conference (NDIA), and submitted paper to MDPI Open Source Systems Journal
Progress (approval, adoption)	• Successfully transitioned from simulation model to hardware-in-the-loop simulation; published paper describing capability in above three venues; demonstrated capability in the Pentagon to SERC sponsor

5.3.5 Systems Engineering for Velocity and Agility Program

The largest challenge facing DoD weapon system development is the need to dramatically accelerate the delivery of new capabilities and new technologies to the warfighter. Systems Engineering is the most direct approach to attacking this challenge. Research projects in this area will develop methods for finding a balance among development speed, system performance, cost and risk. Initial projects will build on work in value-driven design and value-based acquisition. The goal will be a prototype set of methods and processes to bring speed, performance, cost and risk to bear on system design and development decisions from pre-milestone A through every step and every level of system development. Additional research will address the challenges of continuous development and deployment of military capabilities. These include architecting military systems and their development environments to support continuous development, manufacturing and rapid deployment of operational updates; related changes to DoD acquisition and business practices; design of systems to incorporate of user feedback into both the product and development process at all stages; better composability and user tailoring of deployed systems; and means to incorporate better data analytics into military systems to monitor and improve system performance.

Project work in this area will also extend work on agile methods in systems engineering to address a small-team-based approach to rapid and effective system development. Prototype models will be developed to support very rapid design with minimal direction but using tools that support balanced decision making across the development program. This research will be integrated with and follow the digital engineering methods widely adopted in DoD and the digital engineering methods developed by the SERC. Additional research projects will develop prototype models for development speed, cost and risk to support the decision-making models. This research program primarily implements SEMT Strategy 1 above, *Make Smart Trades Quickly*.

Table 5.3-15 offers a description of the *Systems Qualities* Project (SQ), the one current Core-funded project in the *Affordability and Value in Systems* Program.

Table 5.3-15. Projects in the *Systems Engineering for Velocity and Agility* Program

Project	Started	Purpose	Primary SEMT Supported Strategies
Systems Qualities	2012	Pursue the Vision of performing ilities tradespace and affordability analysis for cyber-physical-human systems	1, 4

5.3.5.1 System Qualities (SQ) Project

Table 5.3-16 shows the focus, deliverables, and investment in the Systems Qualities (*SQ)* Project through 2023. The project has three primary components. The Foundations component has pursued three complementary SQ representation approaches. An ontological approach uses DoD stakeholder value propositions to organize means-ends relationships involved in satisfying the stakeholders' value propositions and identifies sources of variability in the SQ values. A semantic approach identifies change-oriented SQs in terms of the semantics of their causes, contexts, agents, and effects. A formal-methods approach uses precisely defined terms to represent the SQs and their relationships. These perspectives have been found to be complementary, and 2018 efforts are proceeding to organize them into a unified framework, and to use the framework to develop guidance for systems engineers to balance tradeoffs among the SQs.

The current initial form of the stakeholder value-based, means-ends framework has Stakeholder Satisfaction as its ultimate objective, and the systems engineering of successful cyber-physical-systems as its domain. It includes the stakeholder values of having current-system Mission Effectiveness (with balanced means of Speed, Delivery Capability, Accuracy, Usability, Scalability, and Versatility); current-system Life Cycle Efficiency (with balanced means of Cost, Duration, Personnel, and other Scarce Quantities, Producibility, and Maintainability); current-system Dependability (with balanced means of Reliability, Availability, Maintainability, Safety, Security, Privacy, Robustness, and Survivability); along with future-system Changeability (with balanced means of Maintainability, Adaptability, and Composability). Further SQs such as Extendibility, Understandability and Testability are lower-level means supporting one or many of the means above.

Table 5.3-16. *System Qualities* Project Timeline

Year	Focus	Key Deliverables
Pre-2019	SQ Ontologies, Maintainability, Technical Debt	Integrated SysE Toolsets, Set-Based Design MPTs, Early Next-Gen Cost Models: SysE, Agility
2019	Cyber-Physical-Human (CPH) System Resilience; Early Continuous Development & Deployment (CD&D) MPTs	Early CPH System Resilience, CD&D MPTs
2020	Scalable, Systems-of-Systems (SoS)-Oriented CPH CD&D MPTs	Scalable, SoS-Oriented CPH CD&D MPTs
2021-23	Annual Experience-Driven Refinements of Scalable, SoS-Oriented CPH CD&D MPTs	Annual Experience-Driven Refinements of Scalable, SoS-Oriented CPH CD&D MPTs

The second primary component involves extending and integrating existing SQ MPTs to better support DoD cyber-physical-human SQ analysis. This includes developing more service-oriented and interoperable versions of current SERC SQ MPTs; developing approaches for better integrating MPTs primarily focused on physical, cyber, or human system SQ analysis; efforts to modify and compose existing SERC SQ MPTs to better interoperate with each other and with counterpart MPTs in the Engineered Resilient Systems (ERS) community and elsewhere; and efforts to apply the MPTs to the SQs tradespace and affordability analysis of increasingly challenging DoD systems.

As Maintainability was key to Life Cycle Efficiency, Changeability, and Dependability, a major 2015-2017 SQ research thrust was devoted to methods, processes, and tools (MPTs) for improving DoD systems Maintainability. The logistics field provided mature support for physical systems Maintainability, but cyber-human system elements' Maintainability support was relatively weak. This led to the development, experimental application, evaluation, and improvements in MPTs for improving the Maintainability of particularly large software-intensive systems. SERC research focused on using cloud services for the automated identification of poor software practices causing Technical Debt (TD); so named due to the fact that the later it was fixed, the more expensive was the fix. These have led to the development of toolsets for tracking the life-cycle increases and decreases of large systems' TD, and to their application in several Navy software safety analyses.

A further workshop on the sources of TD identified a number of non–technical sources of TD. Further analyses of the causes of these sources have led to the development of a framework similar to Technology

Readiness Levels for assessing a system's readiness level for cost-effective Maintainability, called the Software Maintainability Readiness Framework (SMRF), which has been successfully applied on several software systems.

The third primary component focuses on affordability analysis. It addresses the challenges of cost estimation for the next generation of DoD systems, such as costing of more incremental and evolutionary development approaches, of increasingly interdependent systems of systems, of agile development of rapidly fielded systems, of increasingly autonomous systems, and of the tradespace among system costs, deliverables, quality levels, and scope. These have led to the development of the next-generation systems engineering cost model COSYSMO 3.0; an initial model for early requirements-based estimation of agile development costs; and early scoping of a cost model for estimating the cost of increasing levels of software security.

The *SQ* Project transition action plan and characterization are shown in Tables 5.3-17 and 5.3-18 below.

Table 5.3-17. *System Qualities* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	Engage collaborative organizations in DoD (Army Engineer Research and Development Center, TARDEC; Naval Air Systems Command, NAVSEA, Marine Corps, Air Force Aeronautical Systems Center and Space and Missile Systems Command); Industry (major aerospace companies, cost model proprietors), FFRDCs (Aerospace, Software Engineering Institute); Professional/Industry Societies (INCOSE, International Software Engineering Research Network, NDIA) in exploring and prioritizing technical approaches	• Engage Community
2	Organize project into top-priority focus areas: SQ Ontology and Guidance; SQ Models and MPTs; Next-Generation Systems Engineering and Software Cost, and Schedule and Quality Modeling	• Plan Early • Engage Community • Balance Long and Short Term
3	Develop interoperable, service-oriented models and MPTs: converged general, change-oriented, and formal ontologies; interoperable set-based design aids, SysML models and cost estimating tools; Air Force and Navy intelligence, surveillance and reconnaissance UAV models and MPTs; Fact-based multi-Service models and MPTs and Cost-Schedule estimate-range models and MPTs, emphasizing uncertainties and risks.	• Productize • Support Centrally
4	Use workshops, prototypes, and pilots to engage stakeholder communities in exploring, evaluating, and evolving increasingly relevant and practical models and MPTs	• Engage Community • Pilot Continuously

Table 5.3-18. *System Qualities* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• Results of spearheading SQ Community of Interest in identifying, engaging, and collaborating with SQ stakeholders in exploring, evaluating, and evolving increasingly relevant and practical models and MPTs, using evidence-based 4-step plan above.

Characteristic	Evidence
Progress (approval, adoption)	• 269 papers published in the Proceedings of CSER 2014- and 20185, and in INCOSE International Symposia 2014- and 20185. • 18 presentations at NDIA SE Symposia 2014-, 20185. Several presentations at NDIA-Army Ground Vehicle SE and Technology Symposia 2014, 2015. • SERC Best Student Paper 2014; Navy-SERC Best Paper ESEM 2017. • Workshops and tutorials with industry and Government at Aerospace Corp. • Ground Systems Architecture Workshops 2014-, 20185., • Annual COCOMO III and COSYSMO 3.0 workshops and presentations at Army Practical Systems and Software Measurement Users Group Meetings Workshop 2015-2018, • Systems and Software cost modeling presentations at Navy-NGA Cost Modeling Meetings, 2016-2018. • Systems and Software Cost Modeling Forums at the University of Southern California 2014, CMU-SEI 2015, USC 2016,2017, CMU-SEI 2018.

5.3.7 SEMT Area Non-Core Funded Projects

During the initiation of this Technical Plan, the SERC is currently executing six non-Core funded SEMT Area projects as briefly described in Table 5.3-19 below.

Table 5.3-19. SEMT Area Non-Core Funded Projects

Project	Sponsor	Description
Transforming Systems Engineering through Model-Centric Engineering - Phase 5	NAVAIR-NPS	Research on Cross-domain Model Integration, Model Integrity, Ontology, Semantic Web Technologies, MDAO, Multi-Physics Modeling, and Model Visualization has impacts across a broad roll out of functional areas (e.g., Methods, Integrated Modeling Environments, Policy, Contracts & Legal) for the SE Transformation (SET) at NAVAIR. The research is being conducted in the context of NAVAIR SET Surrogate Pilot using collaborative Authoritative Source of Truth levering OpenMBEE, which has been deployed for both NAVAIR and ARDEC to demonstrate art-of-the-possible.
Transforming Systems Engineering through Model-Centric Engineering	RDECOM-ARDEC	Research focused on integrated modeling technologies for ARDEC-relevant domains, including OpenMBEE embodied in SERC-developed Interoperability and Integration Framework (IoIF) for demonstrations across 16 use cases to integrate mission and system models with the ARDEC inspired Decision Framework, a decision ontology based on the Basic Formal Ontology using semantic web technology, with visualizations. Research used five applications to demonstrate MDAO analyses for mission, system and graphical CONOPS.
Verification and Validation (V&V) of System Behavior Specifications	NAVAIR-NPS	NAVAIR SET initiative aims to leverage and extend existing research in the area of Models Processes and Tools for performing early V&V of requirements and architecture models managed within its organization, and to educate its workforce in the use of automated tools for conducting early and continuous V&V across the entire lifecycle.

Project	Sponsor	Description
Framework for Analyzing Versioning and Technical Debt	RDECOM-CERDEC	Use technical debt framework to support best practices for obsolescence management of complete systems. Identify "technical debt" occurrences and their relationships to programmatic and technology-centric decision processes. Develop a plan to ensure the identification, visibility, tracking, and management of "technical debt" across research, materiel development, and sustainment organizational elements. Develop tutorial materials and conduct workshop to transition knowledge of COTS technical debt and associated with mitigation strategies.
Meshing capability	RDECOM-ARDEC	This research is focused on providing a computational model to support the planning cycle injecting relevant threat-based intelligence and operational scenarios into the more traditional capabilities-based planning. The research uses a machine learning - data driven approach, extracting metrics from domain specific texts and creating from them a scenario-based support system for the planning process developed at ARDEC in 2016
Tools and methods framework for ship board power and energy systems	Naval Surface Warfare Center	This project is developing a method for comparing a set of power system architectures relative to a set of high-level capability requirements by capturing qualitative information from subject-matter experts (SMEs) in the decision framework to initiate a requirements decomposition process supporting a power system selection.

5.4 Human Capital Development (HCD)

Over the last decade, the DoD and the defense industrial base have often cited a shortfall in the quantity of systems engineers and in the knowledge, skills, and abilities of those systems engineers[14,15]. Not only is there a critical shortage of systems engineers, but the skillsets and capabilities of these engineers need to rapidly expand to address the growing complexity in the systems they are attempting to engineer. Systems Engineering Vision 2025[16] presents a future view of SE which highlights several areas that directly impact Human Capital Development.

Systems Engineering is not only for those with the title of 'Systems Engineer'. Systems skills are essential for systems decision makers, technical leaders and all engineers. All leaders and those making decisions about systems need to be systems thinkers. Systems thinking skills need to be developed long before graduate studies and should be introduced as early as kindergarten through high school. All engineers should have some education and training in systems and SE. While undergraduate curricula are already full, these skills can be introduced and distilled in cornerstone and capstone projects. Finally, systems engineers need to be well versed in a broad set of socio-technical and leadership skills, serving as a central, multi-disciplinary focal point of systems development with stakeholders of all types.

[14] See http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Documents/Studies/Top%20SE%20Issues%202010%20Report%20v11%20FINAL.pdf.

[15] See http://www.ndia.org/Advocacy/PolicyPublicationsResources/Documents/WSARA-Public-Law-111-23.pdf.

[16] See http://www.incose.org/docs/default-source/aboutse/se-vision-2025.pdf?sfvrsn=4.

Systems engineers will be challenged by the complexity of future systems of systems. The chief engineer who could previously comprehend the workings of a complete system will be challenged to fully understand the behaviors of future systems, creating the need for systems engineering to become more collaborative and data-driven. Organizations are adopting digital engineering methods, processes and tools which will change the nature of systems engineering: it will become more technical and skills with data analytics and information technology management will be at a premium. The ability to rapidly represent systems engineering trades through a combination of established problem-solving methods combined with manipulation of technical data and models will become a core skill base for an established SE. This change process will require active mentoring – linking experienced systems engineers who may be uncomfortable with modeling and software programming to the emerging workforce with more native skills in computer programming and search/access of digital data. In addition, the technology and tools to manage data and models are rapidly evolving, and emergence of machine learning will likely produce several technology revolutions in the data domains over the next several years. This will lead to a transformation of the SE discipline. The vision in systems engineering Human Capital Development (HCD) is to stay at the forefront of these changes and lead the multi-disciplinary development and experience acceleration of future systems engineers.

This change will be further affected by the evolution of digital learning technology. Future education programs should emphasize collaboration, multi-disciplinary challenge problems and introduce case studies that encourage systems thinking. Digital learning platforms will be both an enabler and a challenge – such platforms might emphasize case-based learning, but the SE discipline must also learn the human process of communication and collaboration for holistic problem solving. Experimenting with different digital and collaborative learning environments must be a focus for systems engineering.
The HCD research area directly targets the aforementioned shortfalls and challenges.

5.4.1 HCD Vision and Current Progress

The HCD Vision to achieve the HCD goal is to:

> *Discover how to dramatically accelerate the professional development of highly capable systems engineers and technical leaders in the DoD and the defense industrial base to address the challenges created by the rapidly changing nature of systems, and systems of systems, and the human capabilities necessary to support them, and determine how to sustainably implement those discoveries.*

The goal to achieve this vision is:

> *Ensure a competitive advantage for the DoD and the defense industrial base through the availability of highly capable systems engineers and technical leaders. Aggressively encourage the investigation and use of emerging digital technologies as both a central competency of the future SE and an evolution of SE education.*

Significant HCD progress has been made in the previous SERC Technical Plan through a mix of Core-funded and non-Core funded projects. A number of the successes are described below.

The BKCASE (Body of Knowledge and Curriculum to Advance Systems Engineering) Project has made great strides in organizing information and making it globally accessible and available. This project was successfully completed and transitioned into operation in 2012. Since September 2012, there have been over 1.3 million visits to articles on the *Guide to the Systems Engineering Body of Knowledge* (SEBoK) wiki[17] and a number of universities have adopted all, or part of the recommendations found in the Graduate Reference Curriculum on Systems Engineering (GRCSE)[18]. Their continued use and evolution will provide an up-to-date source for systems knowledge.

The Helix project is showing success in understanding what enables systems engineers to be effective, how systems engineers mature, and in characterizing the systems engineering workforce. Several organizations in government and industry have begun using Helix for their workforce improvement efforts. Uses include utilizing the proficiency model for workforce assessment and planning, and using the standard roles and proficiencies to clarify the expectations for systems engineers.

The *Experience Acceleration (EA)* Program has continued to mature and now has a variety of capabilities that should support experiences in numerous domains and in several different single and multi-player modes. There is a great potential for this technology to advance the strategic objective of educating and training faster. Pilots have been conducted that both show the potential of the technology and have served to provide feedback in its subsequent development. In addition, a set of prototype tools have been developed that show the potential for tailoring existing experiences and developing new ones. Critical work moving forward is in learning evaluation and the validation of the hypothesis that technology can be used to accelerate learning for systems thinking and engineering. This can be facilitated through the use of the EA in Collaborator university courses and training. In addition, it will be necessary to show that experiences can be efficiently created and modified by the non-research community. Finally, a sustaining open source community is needed to ensure that Experience Acceleration experiences and technology can be supported for widespread deployment.

The *Systems Engineering and Technical Leadership Education* Program continues to make strides improving technical leadership and SE education, primarily with non-Core funds. The *Engineering Capstone Marketplace* Project (which is funded by a mix of Core and non-Core funds) is the evolution of research begun in 2010, which showed that a multidisciplinary senior capstone project could enhance development of SE competencies and increase interest in SE. The challenge is in scaling this approach nationwide, to have impact on how thousands of students are taught engineering across the US. The *Technical Leadership* Project also began in 2010 to evaluate the hypothesis that the technical leadership capabilities of high potential, senior DoD systems engineers and technologists could be accelerated through an educational program in technical leadership. This initial research has spawned several efforts for DAU and the Army. The former research resulted in the creation of an innovative approach to educating technical leaders through three lenses: systems, business, and enterprise. That approach was captured in courses have been prototyped, piloted and are being transitioned to DAU. Again, the challenge is in expanding the offering of these courses to broaden their impact.

The *Capstone Marketplace* Program continues to move forward with updates of its website capabilities and expansion of its success to a broader base of project sponsors. The Capstone Marketplace website (www.capstonemarketplace.org) makes it easy for sponsors to reach out to potential students, and it helps students find projects best matched to their interests.

[17] See http://www.sebokwiki.org.
[18] See http://www.bkcase.org.

There are a number of additional remaining gaps that need to be addressed to achieve the HCD Vision. Some of these include: how to better capture the knowledge of systems engineers who are nearing or in retirement, how to more closely couple research results to their dissemination in education and the workplace, and how to expand systems education into kindergarten through high school.

5.4.2 STRATEGIES TO ADDRESS THE HCD VISION

Successfully executing the following strategies will make significant progress towards addressing the HCD Vision:

1. *Create and Provide Easy Knowledge Access: Create and ensure access to critical knowledge and curriculum in emerging gap areas for SE.* Make it easy for systems engineers to understand the SE discipline and to access the information needed to expertly perform SE so that the workforce can master the most important competencies. It is important to take research results and transform them into curriculum and training materials. The world's grand challenges are primarily systems focused. As educators step up to address these challenges, the SE community must lead with the tools and methods of systems engineering and systems thinking.
2. *Improve SE and STEM Education and Training:* Develop recommendations and systems curricula for the next generation of systems engineers, engineers and STEM students. Develop innovative approaches and technology to educate and train systems engineers and systems teams, engineers, and STEM students much more rapidly, effectively and efficiently than with classical means. There are a number of open issues in this area. For example, how do we accelerate learning in critical areas in which there is a shortage of talent, e.g., MBSE, security, mission engineering? How do we influence colleges/universities to change as necessary to support these objectives? Can the DoD help influence these outcomes? Is there an emerging set of people who can help with this? Will there be training in the workplace? The business of education is undergoing a transformation in a connected world, and the SE community can set the pace for these changes.
3. *Develop Effective Technical Leaders and Systems Thinkers:* Develop innovative approaches to educate DoD technical leaders with the right mix of technical, business, and enterprise skills. This will include team building, working with others, facilitation, and virtual collaboration. It will also include development of architectural competence: the ability to understand and act on multiple stakeholder perspectives, communicate a systems view, and conceptualize complex problems and solutions. To address grand challenges, future technical leaders will need a strong understanding of social science, policy, and culture. Finally, in a data-driven world, strong analytical skills and the ability to adapt and learn around computational trades will be at a premium.
4. *Support the Digital Engineering Transformation:* Create a data-driven systems engineering workforce and culture. Systems engineering, as with many enterprise domains, will evolve to be a data driven activity. Big data, analytics, and machine learning are revolutionizing many workplaces through immediate access to information and cross disciplinary collaboration. Systems engineering should not be the exception. Future DE and MBSE initiatives will emphasize the role of systems engineering in managing and governing program digital data across the lifecycle (the authoritative source of truth), and the use of digital models to link hardware and software engineering disciplines to mission objectives. Future engineering data on the desktop will greatly decrease data search time and increase analysis work creating a much more efficient systems engineering workflow. As the transformation occurs, it is expected that the role of the

systems engineer will become much more technical – gradually replacing paper and static presentations with interactive models and visual analytics.

5. *Identify and Address Emerging Gaps:* Track the changes in emerging/critical SE workforce needs, demographics and performance over time necessary to address technological and societal change to determine the advances necessary to satisfy future HCD needs. It is critical to relate the educational challenges posed by the three cross-cutting missions to the educational challenges as is shown in Table 5-4.1.

Table 5-4.1 Educational Challenge Areas posed by SERC Mission Areas

System Evolution	Security	Autonomy
Human-Centered Design	Active Agents (threats)	Prediction & Validation
Lean Processes	Assurance	Agility & Adaptability
Complex Systems Thinking	Software & IT	Human-Machine Interaction
Creative Processes	Social Engineering	AI & Machine Learning
Search-based & Evidence-based	Cyber-Physical Systems	
Need-driven vs. Outcome-driven		
Innovation & Agility		

Three existing and one new HCD research programs directly implement the strategy:

- Evolving Body of Knowledge
- Experience Acceleration
- Systems Engineering and Technical Leadership Education
- Emerging/Critical HCD Areas

5.4.3 Evolving Body of Knowledge Program

This research program primarily implements HCD strategies 1, 2, 3 and 5 above – *Create and Provide Easy Knowledge Access, Improve SE and STEM Education and Training, Develop Effective Technical Leaders and Systems Thinkers,* and *Identify and Address Emerging Gaps*. It includes one current project – Helix. A second project – BKCASE – successfully completed at the end of 2013 as a research effort, although the SERC maintains a role as one of three stewards leading the operation and maintenance of *BKCASE* products. Table 5.4-2 offers a description of these two projects and which strategies they primarily support.

Table 5.4-2. Projects in the *Evolving Body of Knowledge* Program

Projects	Started	Purpose	Primary HCD Supported Strategies
BKCASE	2009; successfully completed at the end of 2013	Though the formal research tasks for BKCASE ended in 2013, the SERC is still engaged in the ongoing effort as a member of the BKCASE Governing Board. In this role, the SERC continues to provide guidance and direction on both SEBoK and GRCSE.	1, 2, 5
Helix	2012	Understand the characteristics of the SE workforce and what enables them to be effective and use those insights to inform workforce development for systems engineers. Using these insights, determine the impact of organizational characteristics – governance, culture, structure – on the workforce's ability to deliver and effective systems engineering capability.	2, 3

5.4.3.2 Helix Project

Helix began in October 2012 to examine the "DNA" of the systems engineering workforce in both DoD and the defense industrial base. From 2012-2016, the project focused on answering three questions:

- What are the characteristics of systems engineers?
- What enables them to be effective and why?
- What are employers doing to improve the effectiveness of their systems engineers?

Based on interviews with over 350 systems engineers and those who work with systems engineers, Helix developed *Atlas*, a theory of what enables systems engineers to be effective. Atlas describes the key proficiencies that impact the effectiveness of systems engineers, the several forces that impact the level of proficiency that systems engineers obtain, how the career paths of systems engineers' progress, how personal and organizational characteristics affect the evolution of systems engineers, and also provides demographic data about systems engineers, such as their typical education and how that demographic data has changed over time. The project included both systems engineers in the defense community and more broadly in such commercial sectors such as healthcare, transportation, and information technology. To date, 23 organizations have participated in Helix.

Starting in 2017, the Helix focus shifted to better understand the context in which systems engineers operate, specifically looking at the organizational characteristics that impact systems engineers' ability to deliver an effective systems engineering capability. The current research questions are:

- How can organizations improve the effectiveness of their systems engineering workforce?
- How does the effectiveness of the systems engineering workforce impact the overall systems engineering capability of an organization?
- What critical factors, in additional to workforce effectiveness, are required to enable systems engineering capability?

The team is looking to add a dozen organizations both inside and outside of the US, expanding the types of participating organizations. The team is also working to specifically structure the sample to include organizations that are approaching systems engineering in ways that differ from the traditional acquisition approaches: rapid fielding, agile, model-based, etc. This will enable the team to provide critical updates to *Atlas* that will provide future direction. The team is also expanding the data collection methodology to utilize surveys and web-based data collection tools. The team is building towards the development of a set of data collection and analysis tools that organizations can use for internal understanding. This information could feed a "flight simulator" that would enable an organization to identify critical areas where systems engineering/systems engineers are being impeded and understand possible methods to address these areas.

Table 5.4-3 shows the focus, deliverables, and investment in the Helix Project through 2018.

Table 5.4-3. *Helix* Project Timeline

Year	Focus	Key Deliverables
Pre-2019	Data collection from a dozen organizations focusing on "non-traditional" systems engineering approaches and improved data collection on organizational characteristics. Analysis of existing data to support modeling.	• Initial models reflecting Atlas findings on systems engineers and organizational characteristics • Web-based data collection tools to improve ease of collection/analysis • Update of Atlas as appropriate • Technical report on progress with plan for 2019
2019	Data collection from 1-2 dozen additional organizations. Update of model(s) to reflect findings. Development of initial "flight simulator" that uses the models/data to provide insight into organizational systems engineering capability, including impacts on the workforce.	• Updated models reflecting Atlas findings on systems engineers and organizational characteristics • Draft "Flight Simulator" • Update of Atlas as appropriate • Technical report on progress with plan for 2020
2020	Finalization of Flight Simulator with guided piloting from at least six organizations	• Final "Flight Simulator" • Final version of Atlas • Technical report
2021-23	To be determined	To be determined

The Helix transition action plan and characterization are shown in Tables 5.4-4 and 5.4-5 below.

Table 5.4-4. *Helix* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	SERC formed an alliance with INCOSE to collaborate broadly on research and then developed a specific agreement to collaborate on Helix; that agreement led to participation from INCOSE's corporate members who provide data, pilot *Atlas*, and aid its adoption.	• Plan Early • Engage Community • Support Centrally
2	Helix has an advisory group from the community and periodically holds workshops with that group and with others to review status, plans, and interim results.	• Engage Community
3	*Atlas* is being piloted with organizations and revised as appropriate.	• Pilot Continuously • Engage Community
4	Helix is gradually creating and validating tools and models to help organizations successfully apply *Atlas* to aid their workforce development.	• Productize

Table 5.4-5. *Helix* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• Activities leading up to Atlas 1.1 (the latest release) were sufficiently useful and practical that several participating organizations have altered their workforce development approaches to accommodate Helix insights.
Progress (approval, adoption)	• Helix has published four technical reports, presented at 21 conferences, held three workshops, and published four journal articles. • Organizations beyond the defense community are participating, expanding Helix outreach.

5.4.4 Experience Acceleration Program

This research program primarily implements HCD Strategy 2 – *Improve SE and STEM Education and Training*. It includes projects aimed at creating automated learning environments that simulate real world experiences of systems engineers. Those experiences should be vivid and realistic to significantly accelerate the learning and maturation of those systems engineers. One project will evolve the current simulation platform, making it ever more robust and capable and enabling quicker and easier construction of new experiences. Other projects will add to the current catalog of experiences, developing new experiences that use the simulation platform. Experiences will vary based on the size and types of systems being acquired, the acquisition lifecycle, the novelty of the technology being acquired, and other parameters of interest. Over the five-year period from 2014-2018, other organizations have joined the SERC in improving the experience platform and in developing additional experiences, creating a marketplace for experience acceleration. Table 5.4-6 offers a description of these projects and which strategies they primarily support. Table 5.4-7 shows the focus, deliverables, and investment in the *Experience Accelerator* Project through 2018.

This program is unusual in that the primary project, *Experience Accelerator*, has had relatively little Core funding. Other DoD and commercial organizations are expected to provide additional non-Core funding to create new Virtual Experiences beginning in 2018.

Table 5.4-6. Projects in the *Experience Acceleration* Program

Projects	Started	Purpose	Primary HCD Supported Strategies
Experience Accelerator	2010	Create the "engine" that will be used to host a wide range of experiences, develop the first virtual experiences that use the engine, and validate the experience accelerator concept through trial use. Keep improving the engine over time as a broader set of experiences are created and trialed with ever more students. Create an open vibrant community that will develop additional virtual experiences that can be shared within the defense industrial base and DoD.	2
Additional Virtual Experiences	Expected 2019 and beyond	Relying on non-Core investment, develop an increasingly broader and richer set of virtual experiences that are hosted on the Experience Accelerator engine	2

Table 5.4-7. *Experience Accelerator* Project Timeline

Year	Focus	Key Deliverables
Pre-2019	Build Experience Accelerator engine, experiences, tools and validate concept in pilots	Experience Accelerator engine, tools and experiences, with pilot results
2019	Develop and pilot "vignette" experiences and update tools	New vignette experiences and updated tools, along with pilot experience results
2020	Migrate Experience Accelerator to open-source support and access model	Website which provides access to Experience Accelerator engine, tools, and experiences with documentation for use
2021-23	Growth of open source community and building a library of experiences	New experiences, increasingly more capable engine and tools, learning evaluations, deployment in marketplace community

The *Experience Accelerator* Project transition action plan and characterization are shown in Tables 5.4-8 and 5.4-9 below.

Table 5.4-8. *Experience Accelerator* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	Worked closely with DAU to determine project concept and scope	• Plan Early
2	Delivered a number of Pilots for instructors and students, updating the Experience Accelerator based on detailed feedback	• Long and Short Term • Pilot Continuously
3	Created Experience Accelerator User Group to publicize results and provide feedback on development. Hold workshops at NDIA SE and INCOSE International Symposium conferences	• Engage Community
4	Develop tools to improve the capabilities of users to customize experiences for their use	• Productize

Table 5.4-9. *Experience Accelerator* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	A number of organizations including the University of Alabama Huntsville, Georgia Tech, AFIT have used the Experience Accelerator for instruction. Industry has also made investments in its use. There are many organizations who are interested in using the technology including the UK MoD which has created an experience. The Experience Accelerator User Group is composed of 16 members from multiple organizations in the Federal Government, FFRDCs, industry and academia.
Progress (approval, adoption)	The Experience Accelerator has undergone several instructor and student pilots at a number of universities and government organizations. Developments are taking place to expand this to corporate institutions. Tools have been developed and piloted with outside organizations which have been used to develop new experiences.

5.4.5 Systems Engineering and Technical Leadership Education Program

This research program primarily implements HCD strategies 2 and 3 – *Improve SE and STEM Education and Training* and *Develop Effective Technical Leaders*. It currently includes one primary projects: the *Engineering Capstone Marketplace* Project. The *Capstone* Project has mixed Core and US Special Operations Command funding.

Table 5.4-10 offers a description of these projects and which strategies they primarily support.

Table 5.4-10. Projects in the *Systems Engineering and Technical Leadership Education* Program

Projects	Started	Purpose	Primary HCD Supported Strategies
Engineering Capstone Marketplace	2010	Originally intended to show how to conduct multidisciplinary senior capstone projects in classical engineering programs, especially those that increase awareness of and appreciation for DoD applications. Building on its early success, the project has morphed into a marketplace where companies and government organizations can post on a website problems suitable for senior capstone projects. Students from multiple universities form teams to work on those projects under the supervision of faculty and the posting organization. Although small today, this marketplace model has the potential to scale nationwide, involving thousands of students in hundreds of projects and universities.	2
Technical Leadership	2010	Develop innovative ways to teach technical leadership to the DoD acquisition workforce, including not only systems engineers, but also others who must understand technical leadership, such as program managers. Iteratively pilot the resulting courses and integrate them into the DAU curriculum.	2,3

5.4.5.1 Engineering Capstone Marketplace Project

The *Engineering Capstone Marketplace (ECM)* Project has evolved since the start of research in 2010, which showed that multidisciplinary senior capstone projects can enhance development of SE competencies and increase interest in SE among undergraduate students. *ECM* is now in its eighth year, matching engineering students starting their senior design projects with DoD sponsors providing challenging real-world problems, dedicated mentors, and subject matter experts. The Capstone Marketplace is the connective medium which showcases challenging problems, attracting the interests of universities and their undergraduate teams. DoD project sponsors provide funding for student research, materials, prototyping, testing, and project related travel. Capstone Marketplace managers help identify problems which are best suited to multi-disciplinary approaches. Government client representatives act as team advisors and subject matter experts. They are also the "customers" in a sequence of system-level design reviews. Marketplace personnel provide the teams with high level guidance on engineering processes and techniques as requested. The SERC Capstone Marketplace is distinct from other university capstone events. The Marketplace is a portal where students and instructors can connect with real customers who have real problems; the value of direct interaction with "end users" is often extremely high.

The website, its processes, customer base, and funding resources have recently been expanded, part of an ongoing effort to scale up the Capstone Marketplace experience to a broader university audience. Some recent changes include: use of Firm Fixed Price contracts, inclusion of non-SERC universities in Capstone work, and the addition of key management staff. The Marketplace enjoys growing relationships and support from government organizations, including USSOCOM and the DOD's Rapid Response Technology Office. Other government agencies, including the U.S Coast Guard, are joining the Marketplace with their research topics.

Government sponsors have received many useful results from Capstone Marketplace projects. Several projects have led to follow on development and production efforts. These items could not have reasonably been developed elsewhere without substantial resource investments. Students participating in Capstone Marketplace projects are enhancing their understanding and skill in SE activities and becoming the future government and industry engineering workforce.

Table 5.4-11 shows the focus, deliverables, and investment in the *ECM* Project through 2018.

Table 5.4-11. *Engineering Capstone Marketplace* Project Timeline

Year	Focus	Key Deliverables
Pre-2019	Expansion of Capstone Marketplace to a nation-wide network of technical universities	Streamlined academic, technical, contracting, and acquisition policies and procedures. A robust infrastructure of people, processes, and tools in the Capstone Marketplace coordinating and managing large-scale involvement of universities, students, and organizations Active Capstone research work at 6 or more universities
2019	Bringing "whole of government" to the Capstone Marketplace	3 or more government agencies participating in the Capstone Marketplace. Use of USSOCOM's "Vulcan" application and other standardized government tools for technology coordination and networking.
2020	Introduction of advanced SE projects in Capstone work at the graduate level.	Expansion of the Capstone Marketplace experience to university graduate level engineering curriculums.
2021-23	Maturation of the Capstone Marketplace as a self-sustaining "service" enterprise, managed for government benefit	Industry participation, along with multiple government organizations and agencies, generating Capstone topics, assisting student Capstone teams, and supporting and resourcing the Capstone Marketplace.

The *ECM* Project transition action plan and characterization are shown in Tables 5.4-12 and 5.4-13.

Table 5.4-12. *Engineering Capstone Marketplace* Project Transition Action Plan

#	Transition Action	Principles Implemented
1	The transition of the *ECM* from an internal SERC capability to a stand-alone website that can be readily transitioned was part of the project goals which were refined in 2014. Steps that have been taken in the regard include; registration of a non-SERC domain name www.capstonemarketplace.org, outreach to the academic capstone design community, website redesign to reduce administrative load, development of web-site resources that better enable users to manage, plan, and conduct their projects.	• Plan Early • Long and Short Term • Productize
2	Outreach to both of the key national capstone project user groups have been conducted with participation and distribution of *ECM* literature at NDIA events, publication and presentation of an *ECM* paper and distribution of *ECM* literature at the 2015 American Society for Engineering Education (ASEE) conference. Various other efforts to engage government sponsors for *ECM* projects continue. Development of *ECM* project briefing materials is ongoing.	• Engage Community
3	Results of recently completed *ECM* student projects along are being assessed. Outreach to faculty advisors and sponsor liaisons to review results and determine lessons learned are ongoing.	• Pilot Continuously
4	A plan to develop online tools for the *ECM* website that will better enable dissemination of basic SE tools and processes and assessment of SE learning is being developed.	• Long and Short Term • Engage Community

Table 5.4-13. *Engineering Capstone Marketplace* Project Transition Characteristics

Characteristic	Evidence
Readiness (relevance, practicality)	• 40 DOD and USCG research topics have been posted on the Capstone Marketplace website for academic year 2018-2019. Approximately 25 student teams at 10 universities will be engaged on these problems. This represents a 6X expansion of capstone activities over the previous academic year. Increased university and government sponsor interest in capstone opportunities are strong signs of rapid future year growth.
Progress (approval, adoption)	• U.S. Special Operations Command's Science and Technology Directorate has been the mainstay of sustaining and growing the Capstone Marketplace activities. • 2 conference papers have been published including a recent publication and presentation to the ASEE Design in Engineering Education Division. It is this group that is the most likely to adopt the *ECM* as a resource for faculty and students. This group has agreed to link the *ECM* to their Capstone Design Hub website and disseminate information on the *ECM* to its members. • Briefings on the Marketplace to other professional societies continues, including an upcoming presentation to National Defense Industrial Association's System Engineering Conference

5.4.6 Emerging/Critical HCD Areas Program

This research program primarily implements HCD Strategy 2 and 5, *Improve SE and STEM Education and Training* and *Identify and Address Emerging Gaps*. It currently includes several primary projects: *Systems Engineering Research Needs and Workforce Development Assessment*, *Mission Engineering Competencies*, and *Human Capital Development- Resilient Cyber-physical Systems*. Each of the projects noted below are exploratory in nature and designed to determine the needs for future HCD research, thus, in depth descriptions and roadmaps for each are not included in this Technical Plan.

Table 5.4-14 offers a description of these projects and which strategies they primarily support.

Table 5.4-14. Projects in the *Emerging/Critical HCD Areas* Program

Projects	Started	Purpose	Primary HCD Supported Strategies
Systems Engineering Research Needs and Workforce Development Assessment	2017	This research task is engaging with Department of Defense Science and Technology (DoD(S&T)) and Engineering leaders across the DoD's laboratories and engineering centers to identify inclusive discernable patterns with regard to long-term, comprehensive research priorities and opportunities for impact, centering on an assessment of systems engineering research needs and the workforce development.	2,5
Mission Engineering Competencies	2017	This research task focuses on the exploration of the current state of mission engineering and developing the foundations for a mission engineering competency model. The task is using literature reviews and grounded theory based on the HELIX project to document and project critical skills for successful mission engineering.	2,5
Human Capital Development- Resilient Cyber-physical Systems	2017	This research task focuses on a survey of the current state of academic curricula and educational programs in the U.S. related to security and trust in cyber-physical systems (CPS). In particular the research addresses the needs for system security in the types of large-scale CPS frequently developed in the defense domain, which can be characterized as unique physical platforms utilizing custom and off-the-shelf hardware and software components with connectivity to information and communications technologies.	2,5

5.4.7 HCD Area Non-Core Funded Projects

During the time of the past Technical Plan, the SERC executed four non-Core-funded HCD Area projects. However, there are currently no HCD projects being funding with non-Core funds.

5.5 Infrastructure Development

The SERC Vision states, in part, that at the end of this 5-Year plan:

- The SERC operates the world's largest and most-visited *SE Research Web site*, including the largest and best-organized SE Research experience base.
- It continues to provide leadership in evolving the SE Body of Knowledge.
- It runs the most widely attended and highest-rated SE Webcast series.

The SERC will develop the infrastructure that can be used by all of the research programs to support achieving these elements of the Vision. The strategy is to focus on two specific areas: the SERC Website and the SERC Innovation and Demonstration Lab. This work is scoped to be accomplished through a mix of SERC investment funds and Core funds.

5.5.1 SERC Website

The SERC website is intended to become the world's premier SE research website and researcher collaboration portal. As stated in the SERC vision, it is intended to become "the world's largest and most-visited SE Research website, including the largest and best-organized SE Research experience base". To support this objective, the SERC website is being redesigned in 2018 and has regular changes, additions and improvements. Through a simple, clean, and intuitive web interface, site visitors can:

- Learn about the SERC;
- View news and events, not just SERC-related but those relevant to the entire SE community;
- Review and download current and historical SERC publications, including annual reports, technical plans, research papers, technical reports, and associated articles;
- View presentations from past SERC events, including SERC Sponsor Research Reviews and Doctoral Students Forums;
- Gain an understanding of SERC-affiliated programs, such as the SERC Doctoral Fellows Program; and
- With appropriate credentials, log in to the SERC Collaboration Portal, File Storage, and Product Distribution environment.

All of this functionality exists on the current SERC website with the exception of the collaboration portal, file storage, and product distribution environment. The remaining functions will be implemented in concert with the development of the SERC Innovation and Demonstration Lab (SIDL) described in the next section. Initial operational capability of the portal with updated capabilities is anticipated in 2018.

5.5.2 SERC Innovation and Demonstration Lab (SIDL)

As mentioned earlier, one of the SERC's major goals for 2018 is to operate the world's largest and most-visited *SE Research Web site*, including the largest and best-organized SE Research experience base. Rather than strictly share written materials, the SERC will share its MPTs with the systems research community. The SIDL and the SERC Website will be the primary vehicles for these collaboration and sharing efforts.

The SIDL will be the first stop for an SE researcher. The virtual face of the facility will be integrated within the SERC website, effectively acting as a repository for the source code, executable files, data files, technical reports, white papers, and documentation developed and matured as part of SERC research. In addition, the site will contain a description of MPTs along with online demonstrations, videos, instructions, and downloads for SERC developed tools, open source tools, and URLs of often-used commercial tools. This material will be appropriately linked to the reports, papers, and other documentation relating to SERC sponsored research. At a future date, this may be linked to non-SERC sponsored SE research as well. Wikis and chat rooms will provide the means by which SE researchers can share their experiences with these tool sets. Another possibility for a SERC hosted and distributed tool is a Linux distribution packaged with all available open source SE tools that can run in this environment. This software could be made available as a downloadable "SE research starter kit." The SERC would provide expertise and assistance to SERC collaborating researchers to ensure that their research tools, data, and results are shareable on the SIDL.

The central physical facility is currently at Stevens Institute of Technology as an immersive environment in which SERC researchers can dynamically visualize their data, test hypotheses, develop appropriate algorithms and associated MPTs, and draw conclusions. The SIDL provides a means to "package" and "serve" demonstrations on demand, meaning that all configurations and settings are stored within the demonstration "package." So, when one demonstration requires specific settings in the Lab, it will not conflict with another demonstration's settings or lab configuration requirements. The facility consists of multiple vertically-mounted touchscreen displays along with the necessary computer hardware to run simulations and drive the graphical environment. Beyond the hardware and software, this lab is designed to provide multiple benefits to the SERC researchers and staff. The SIDL also provides a means for SERC researchers to collaborate remotely and "come together" in a lab environment. Additional physical facilities of various capabilities will be supported at other SERC collaborating institutions. These facilities will be supported by their host collaborating institutions but will provide an environment to demonstrate SERC research to interested parties near those sites.

6 NEW PROJECT INITIATION

There are numerous sources for new SERC projects. In many instances, the government sponsors have emerging critical problems that require the insights of research efforts. In these cases, an open call may be made to solicit proposals from within the SERC collaborator base to find the best research ideas. These are often reviewed by SERC leadership, the SERC Research Council, and the government sponsors. In other cases, the sponsor may have already identified leading researchers for the efforts to write a proposal for the work. In both approaches, the SERC strives to form collaborative teams when it is appropriate. The research community may develop research concepts that are presented to various federal sponsoring agencies, some of which may choose to sponsor the research. Each research program also develops new research topics that are related to their ongoing research efforts. Finally, the SERC has initiated a formal process of incubation grants to provide funding for SERC collaborators so that they can develop their research ideas to the point where formal proposals can be made. Research ideas from the incubation grants are described below.

As described in this Technical Plan, the SERC typically performs research on 20 to 25 active tasks simultaneously, exploring well-defined topics that are aligned with the SERC's research strategy. While it is believed that that the aforementioned research programs have a great potential to have a transformative impact on the DoD, IC, and beyond, there is a need to support new ideas in their infancy that may become critical research programs for emerging challenges. This "incubation" capability is supported by an annual open call to the SERC research collaborating universities to propose early stage research that can be nurtured through relatively small levels of seed funding.

The initial open call for the first incubation grant took place in September 2014 with the objective of identifying and developing several short white papers outlining research programs with a significant potential to improve the practice of engineering systems. A total of 29 responses were received and reviewed with the sponsor and SERC Research Council. Of these, five proposals were selected and funded. This process was repeated with an open call that took place in December 2016. A total of thirty responses were received and reviewed with the sponsor and the Research Council. Of these, the following seven proposals were selected and funded as Incubator Projects, while those shown were chosen for funding and are included in this Technical Plan:

1. Paul Grogan, Stevens Institute of Technology, *Game-theoretic Risk Assessment for Distributed Systems (GRADS)*
2. Karen Marais, Purdue University, *Data Science Approaches to Prevent Failures in Systems Engineering*
3. Val Sitterle, Georgia Tech, *Systemic Security and the Role of Heterarchical Design in Cyber-Physical Systems*
4. Lu Xiao, Stevens Institute of Technology, *Identifying and Measuring Modularity Violations in Cyber-Physical Systems*

The results of these efforts will be considered for Core funding and potentially non-Core funding as well. Future calls are scheduled on a biennial basis, in 2020 and 2022.

ACRONYMS AND ABBREVIATIONS

ABET - Accreditation Board for Engineering and Technology

AIAA - The American Institute of Aeronautics and Astronautics

ASEE – American Society for Engineering Education

AWB – Analytic Workbench

BBP – Better Buying Power

BKCASE – Body of Knowledge and Curriculum to Advance Systems Engineering

CMU – Carnegie Mellon University

CONOPS or ConOps – Concept of Operations

CRADA – Cooperative Research and Development Agreement

CSER – Conference on Systems Engineering Research

DATASEM – Demonstration and Analysis Tool for Adaptive Systems Engineering Management

DAU – Defense Acquisition University

DoD – Department of Defense

DSL – Domain Specific Language

EA – Experience Accelerator

ECM – Engineering Capstone Marketplace

ERS – Engineered Resilient Systems

ESOS – Enterprises and Systems of Systems

FACT – Framework for Assessing Cost and Technology

FFRDC – Federally Funded Research and Development Center

FILA-SoS – Flexible and Intelligent Learning Architectures for Systems of Systems

GRCSE – Graduate Reference Curriculum for Systems Engineering

HCD – Human Capital Development

IC – Intelligence Community

IEEE-CS – Institute of Electrical and Electronics Engineers Computer Society

IMCSE – Interactive Model-Centric Systems Engineering

INCOSE – International Council on Systems Engineering

JHUAPL – Johns Hopkins University Applied Physics Lab

KSS – Kanban Scheduling System

MBSE – Model-Based Systems Engineering

MPT – Method, Process, and/or Tool

MS-SE – Masters Degree in Systems Engineering

NAVSEA – Naval Sea Systems Command

NCSOS – Net-Centric Systems of Systems

NDIA – National Defense Industrial Association

NIST - National Institute of Standards and Technology

NSWC – Naval Surface Warfare Center

OSD – Office of the Secretary of Defense

PhD-SE – Doctor of Philosophy Degree in Systems Engineering

PI – Principal Investigator

QSAM - Quantitative Schedule Acceleration Model

QTR – Quantitative Technical Risk

SE – Systems Engineering

SE&M – Systems Engineering and Management

SEBoK – Systems Engineering Body of Knowledge

SEEK – Systems Engineering Expert Knowledge

SEMT – Systems Engineering and Systems Management Transformation

SERC – Systems Engineering Research Center

SIDL – SERC Innovation and Demonstration Laboratory

SOF – Special Operations Forces

SoS – System of Systems

SoSE – System of Systems Engineering

SQ – System Qualities

STEM – Science, Technology, Engineering, and Math

SysML – Systems Modeling Language

TARDEC – Tank and Automotive Research, Development, and Engineering Center

TS – Trusted Systems

UARC – University Affiliated Research Center

USNWR – US News and World Report

USD(AT&L) – Undersecretary of Defense for Acquisition, Technology & Logistics

USD(R&E) – Undersecretary of Defense for Research and Engineering