2019
RESEARCH TRANSITION REPORT

Transitioning research into practice -
crossing boundaries through integrative collaboration

SYSTEMS ENGINEERING RESEARCH CENTER

TABLE OF CONTENTS

ABOUT THE SERC

The Systems Engineering Research Center (SERC), a University-Affiliated Research Center (UARC) of the United States Department of Defense, leverages the research and expertise of senior lead researchers from 22 collaborator universities throughout the United States. The SERC is unprecedented in the depth and breadth of its reach, leadership, and citizenship in systems engineering through its conduct of vitally important research and the education of future systems engineering leaders.

Led by Stevens Institute of Technology and principal collaborator the University of Southern California (USC), the SERC launched in 2008 as a national resource providing a critical mass of systems engineering researchers—a community of broad experience, deep knowledge, and diverse interests. SERC researchers have worked across a wide variety of domains and industries and bring that wide-ranging wealth of experience and expertise to their research. Establishing such a community of focused SE researchers, while difficult, delivers impact well beyond what any one university could accomplish.

OBJECTIVE OF THIS RESEARCH TRANSITION REPORT

All research within the SERC is conducted with an objective of transitioning that research into practice, as appropriate. This aspect of the SERC continues to grow in impact through our collaboration with a number of FFRDCs, National Laboratories, and DoD Industry. To support the SERC transition goals, this report highlights research tasks completed in the government fiscal year 2019 (GFY2019), from 1 October 2018 - 30 September 2019. SERC researchers have published more than 450 technical papers and reports over the past eleven years. Research findings have transitioned into numerous courses across the SERC universities and beyond. We encourage organizations to review the research tasks highlighted in this report, and to contact us if we can assist in the necessary discussion and engagement to support the transition of relevant research into practice at *info@sercuarc.org*.

INTRODUCTION AND CONTEXT

The SERC mission is to enhance and enable the DoD's capability in systems engineering for the successful development, integration, testing, and sustainability of complex defense systems, services, and enterprises. This is done through research leading to the creation, validation, and transition of innovative SE methods, processes, and tools (MPTs) to practice. It responsibly manages impact while evolving and coalescing the number, connectedness, and responsiveness of the SE research community in the United States to the needs of the DoD.

In coordination with its sponsors, the SERC has focused its research portfolio into four thematic areas with associated Grand Challenges, as shown in Figure 1 and described.

Figure 1. Research Areas Addressed by SERC Research Tasks

Enterprises and Systems of Systems

Human Capital Development

Systems Engineering and Systems Management Transformation

Trusted Systems

ENTERPRISES AND SYSTEMS OF SYSTEMS:

Providing ways to develop, characterize and evolve very large-scale systems composed of smaller systems, which may be technical, socio-technical, or even natural systems. These are complex systems in which the human behavioral aspects are often critical, boundaries are often fuzzy, interdependencies are dynamic, and emergent behavior is the norm. Research must enable prediction, conception, design, integration, verification, evolution, and management of such complex systems.

> ***Grand Challenge:*** *Create the foundational SE principles and develop the associated MPTs that enable the DoD and its partners to model (architect, design, analyze), acquire, evolve (operate, maintain, monitor, adapt) and verify complex enterprises and systems of systems to generate affordable and overwhelming competitive advantage over its current and future adversaries.*

HUMAN CAPITAL DEVELOPMENT:

Providing ways to ensure that the quality and quantity of systems engineers and technical leaders provide a competitive advantage for the DoD and defense industrial base. Research must determine the critical knowledge and skills that the DoD and IC workforce require as well as determine the best means to continually impart that knowledge and skills.

> ***Grand Challenge***: *Discover how to dramatically accelerate the professional development of highly capable systems engineers and technical leaders in the DoD and defense industrial base and determine how to sustainably implement those discoveries.*

SYSTEMS ENGINEERING AND SYSTEMS MANAGEMENT TRANSFORMATION:

Providing ways to acquire complex systems with rapidly changing requirements and technology, which are being deployed into evolving legacy environments. Decision-making capabilities to manage these systems are critical in order to determine how and when to apply different strategies and approaches, and how enduring architectures may be used to allow an agile response. Research must leverage the capabilities of computation, visualization, and communication so that systems engineering and management can respond quickly and agilely to ensure acquisition of the most effective systems.

> ***Grand Challenge:*** *Move the DoD community's current systems engineering and management MPTs and practices away from sequential, document-driven, hardware-centric, point-solution, acquisition-oriented approaches; toward concurrent, portfolio and enterprise-oriented, hardware-software-human engineered, model-driven, set-based, full life cycle approaches. These will enable much more rapid, flexible, scalable definition, development and deployment of the increasingly complex, cyber-physical-human DoD systems, systems of systems and enterprises.*

TRUSTED SYSTEMS:

Providing ways to conceive, develop, deploy and sustain systems that are safe, secure, dependable, adaptable and survivable. Research must enable prediction, conception, design, integration, verification, evolution and management of these emergent properties of the system as a whole, recognizing these are not just properties of the individual components and that it is essential that the human element be considered.

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

TRANSITION APPROACH

The SERC approaches transition in a number of ways, beginning when the research effort is first defined. 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 the SERC providing real systems engineering research value to its sponsors.

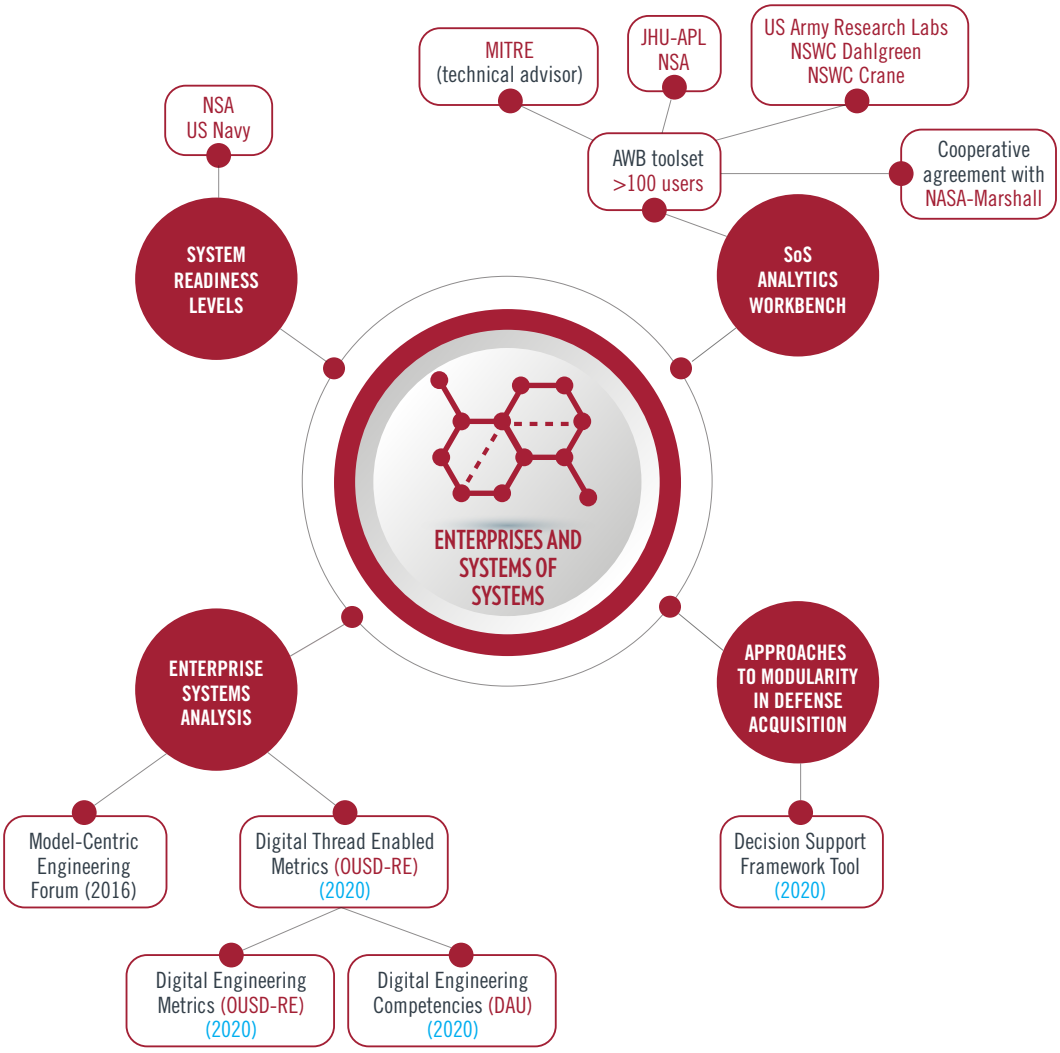
Major impact is realized when the MPTs are transitioned to the early majority. A SERC MPT successfully transitioned to the early majority would be:

- 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

As the SERC has continued to grow and mature, 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. As the graphics on the following pages depict, strong relationships have been forged with several professional organizations, including INCOSE and the National Defense Industrial Association (NDIA) Systems Engineering Division to name a few. The following graphics depict the history of SERC throughout each of the research areas.

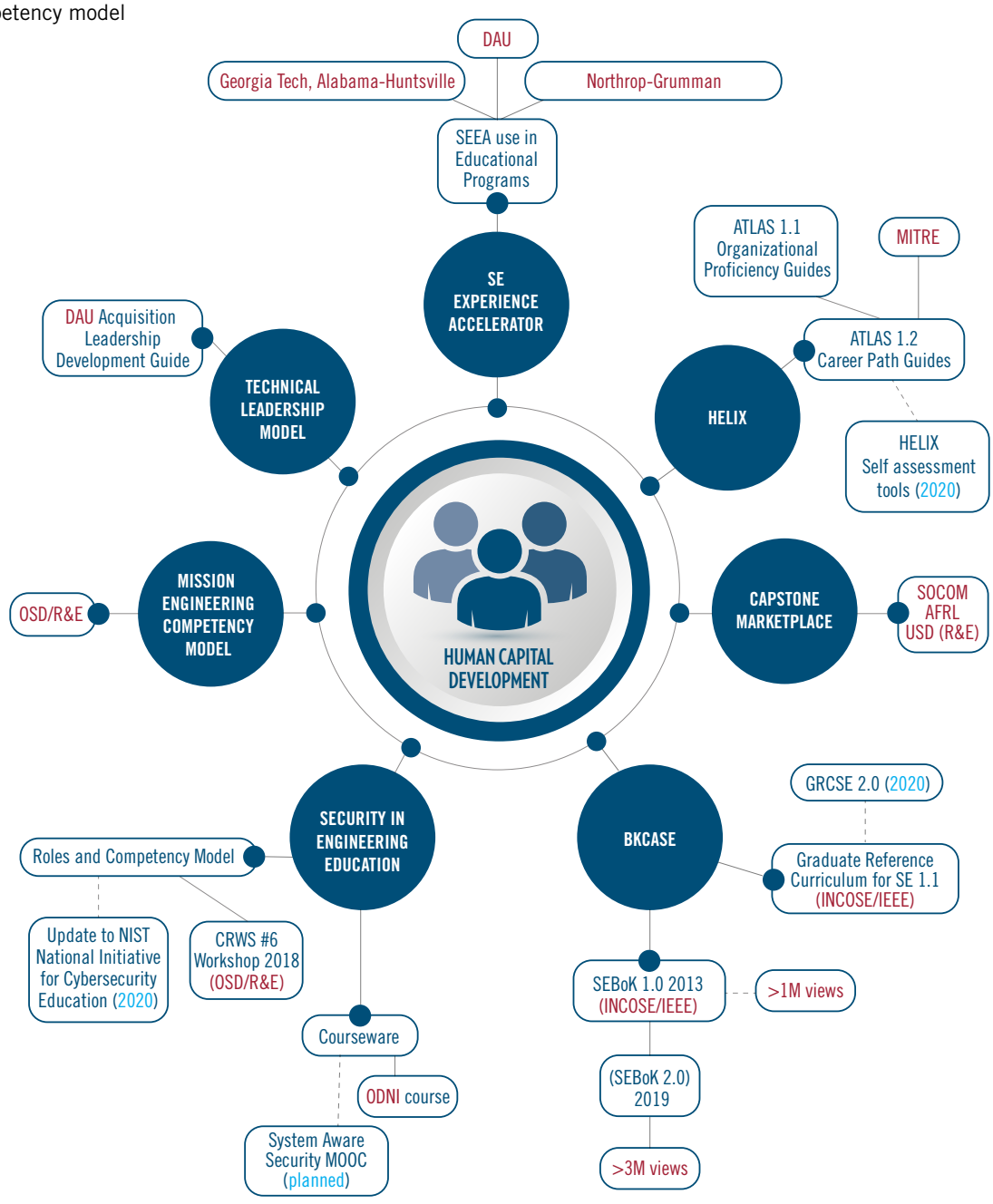
ENTERPRISES AND SYSTEMS OF SYSTEMS:

- With MITRE as a technical advisor, the SoS Analytics Workbench tool set has over 100 users and has collaborated broadly with JHU-APL NSA, US Army Research Labs as well as a Cooperative agreement with NASA-Marshall
- The concepts and methods for calculating System Readiness Levels were developed along with NSA and US Navy and are now used regularly by those organizations.
- Approaches to plan strategy and assess measures for enterprise transformation developed in the Enterprise Systems Analysis research were first applied to healthcare and then to DoD policy including DoD acquisition enterprise transformation using Digital Engineering. Current work is being conducted to support OUSD-RE in the areas of Digital Engineering Metrics, Digital Model Curation, and with DAU in Digital Engineering Competencies.



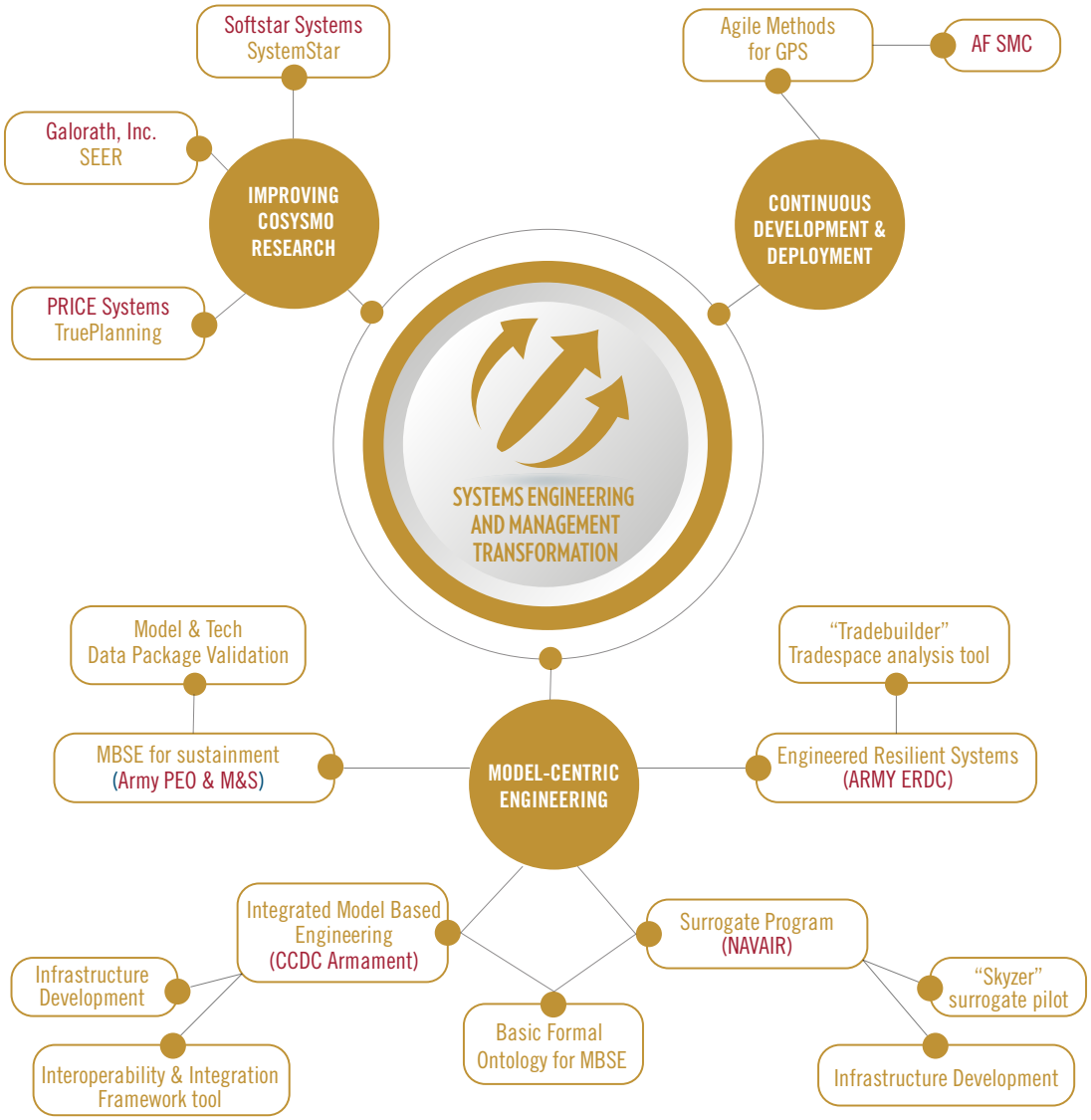
HUMAN CAPITAL DEVELOPMENT:

- The SE Experience Accelerator is being used by several universities in their masters level SE programs. The DAU and Northrop Grumman are also using the game-based simulator in the delivery of their educational programs
- The Helix study developed the Atlas 1.1 SE career path guide, and Atlas 1.2 organizational proficiency guide. HELIX has been adopted by MITRE as well as several commercial companies. HELIX development is continuing with the development of web-based self-assessment tools
- The SERC Capstone Marketplace engages with undergraduate students in SE research across the SERC network and beyond. In 2019 the project supported 28 senior design teams across 10 universities, involving ~150 students
- The BKCASE project developed a body of knowledge for SE. The project developed the SEBoK website which is maintained jointly between the SERC, INCOSE, and IEEE. SEBoK has earned over 3 million views to date. The project also developed the Graduate Reference Curriculum for SE 1.1 used by a number of universities, with version 2.0 anticipated in 2020
- The SERC has made substantial impact in Security in Engineering Education through courseware development. The work was published at a DoD Security in Engineering Education workshop in 2018 and is working to develop a competency model



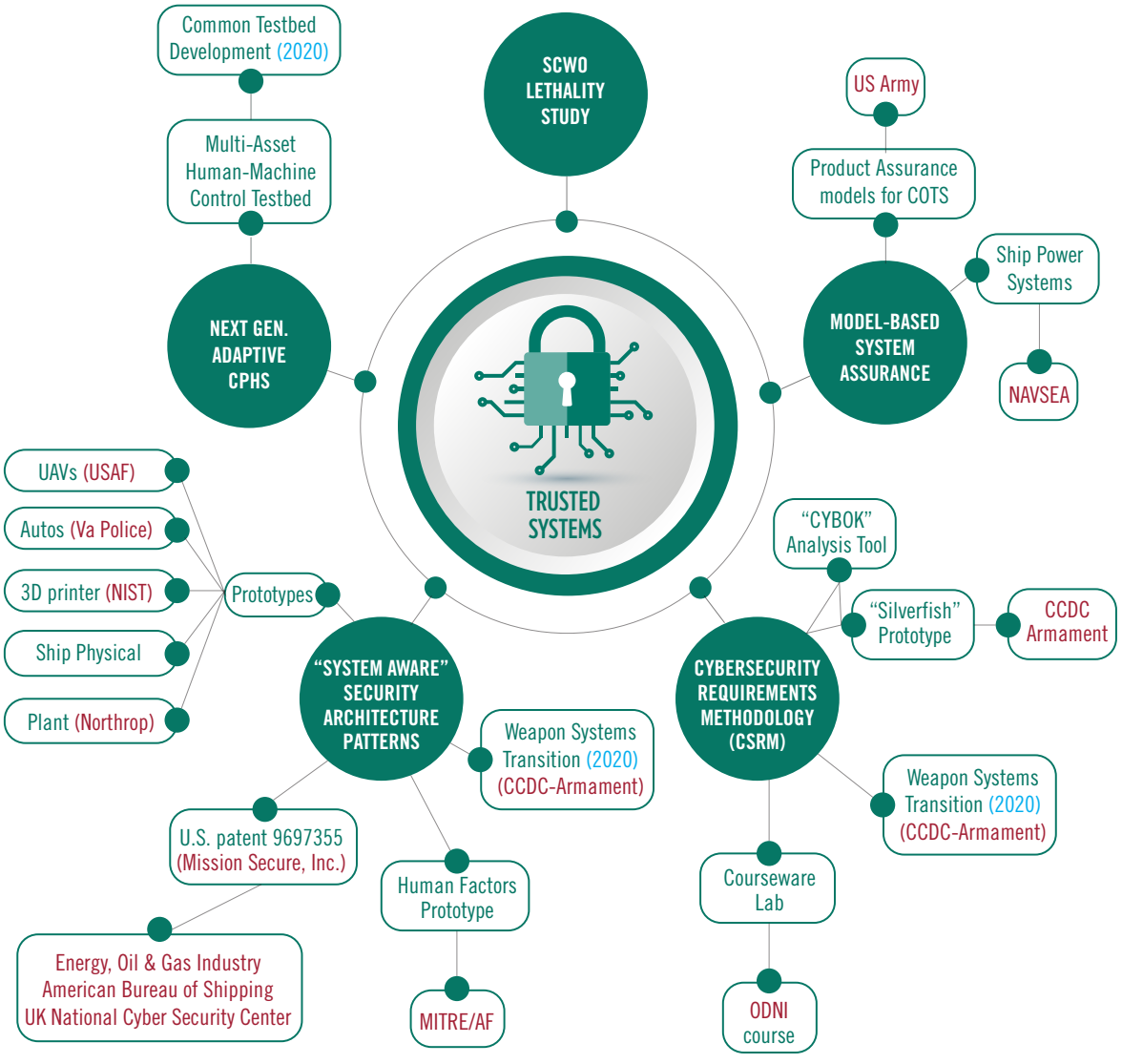
SYSTEMS ENGINEERING AND SYSTEMS MANAGEMENT TRANSFORMATION:

- Extensive transition work is represented in the area of Model-Centric Engineering, specifically a Surrogate Program with NAVAIR, Engineered Resilient Systems with Army ERDC, Integrated Model Based Engineering with CCDC AC, and MBSE for sustainment with Army PEO. Areas of transitioned research include tradespace analysis tools that use Multi-Domain Analysis and Optimization (MDAO), set-based design, basic formal ontology for MBSE, integration of model-management tools, use of MBSE for program source selection
- The SERC has supported a number of projects for improving COSYSMO, the standard toolset for estimation of SE effort in large projects. SERC COSYSMO projects are transitioned to several industry partners who provide SE effort estimation tools
- In the area of Velocity, the SERC hosted a DoD workshop on Continuous Development and Deployment of military capabilities, and is transitioning SE principles for agile methods to the DoD GPS program

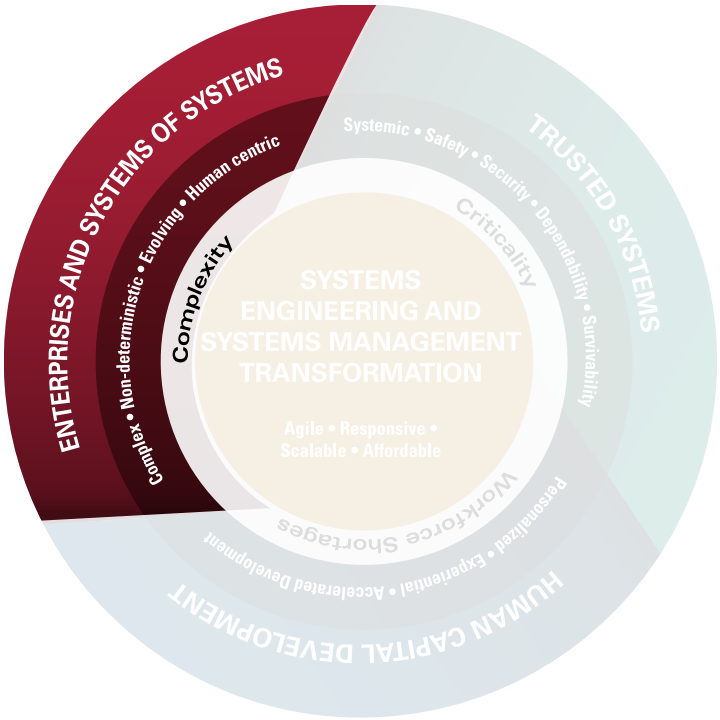


TRUSTED SYSTEMS:

- SERC "System Aware" Security Architecture Patterns, a methodology to design in security for cyber-physical systems, has resulted in various prototypes for the USAF, Virginia police department, NIST, Northrop Grumman and MITRE/AF. A portion of the toolset was patented and transitioned to the Oil and Gas and Shipping domains. in addition, methods are now being employed in a full Weapon System Transition with CCDC AC.
- As part of the System Aware security work, the SERC standardized a Cybersecurity Requirements Methodology. Transition activities include a course developed for the ODNI, a CYBOK analysis tool and "silverfish" prototype for CCDC AC. The methodology is informing future research across the SERC and is being extended by teams at Stevens, UVa, and Georgia Tech
- These efforts continue to promote Model-Based System Assurance as a key enabler for future more secure systems. Additional transition has been done through Product Assurance models for the US Army and NAVSEA
- The SERC led a Super Critical Water Oxidization Lethality Study that brought together leading researchers across the SERC *collaborators who are renowned for their work in safety and security. This is an example of SERC thought leadership in an important DoD study*
- *Recently, SERC researchers at USC transitioned a Common Testbed and Development environment for experimentation with Next Generation Adaptive Cyber-Physical-Human Systems to the Aerospace Corp. This is a simulation environment allowing planning and algorithm development for human-machine teaming*



ENTERPRISES AND SYSTEMS OF SYSTEMS



Providing ways to develop, characterize and evolve very large-scale systems composed of smaller systems, which may be technical, socio-technical, or even natural systems. These are complex systems in which the human behavioral aspects are often critical, boundaries are often fuzzy, interdependencies are dynamic, and emergent behavior is the norm. Research must enable prediction, conception, design, integration, verification, evolution, and management of such complex systems.

ESOS Area Goal: *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.*

One research task in the ESOS area is highlighted in this transition report:

- *Healthcare*

RESEARCH COUNCIL MEMBERS FOCUSED ON THIS THEMATIC AREA:

Daniel A. DeLaurentis

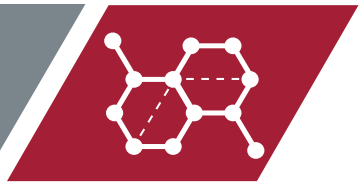
Chief Scientist, SERC Professor, Director, Chief Scientist, Institute for Global Security and Defense Innovation (i-GSDI), Purdue University

William B. Rouse

Senior Fellow, Office of Sr. Vice President for Research, McCourt School of Public Policy, Georgetown University

Oliver de Weck

Professor of Aeronautics and Astronautics, Massachusetts Institute of Technology



HEALTHCARE

Principal Investigator: ***William Rouse***
University: ***Georgetown University***

Investments in RT 41, 44, 110, 138, and 161 have led to broadly applicable enterprise modeling capabilities. These capabilities have been applied to addressing problems and issues in national security, healthcare delivery, and higher education.

Healthcare applications have been funded by CMS and RWJF, as well as MITRE. A major National Academies (Engineering and Medicine) initiative on cancer control, strongly based on this research, was recently briefed to Senate and House Committees. Major healthcare providers involved have included Emory Health, Indiana Health, Johns Hopkins, Mayo Clinic, MedStar, Mt. Sinai, Northwell Health, Penn Medicine, Piedmont Health, Sloan Kettering, and Vanderbilt Health. Curis Meditor and Northern Light are leading commercial spin-offs of these capabilities.

Higher education applications of capabilities supported by SERC have resulted in a book, a high profile PNAS article, and a recent major presentation at the Swedish Embassy. George Mason University, Georgia Tech, IIT (Hyderabad), Indiana University, MIT, Northwestern, NSF, St Johns, University of California (Merced), University of Massachusetts, University of Maryland, and University of Michigan have downloaded the computational model we developed. We have recently been working to extend this model to include a behavioral economic model of students' decision making, particularly with regard to American students deciding to pursue graduate STEM degrees. The American Society for Engineering Education will soon record a video program highlighting this research for distribution to its 400 university members and 50 corporate members.

These healthcare and education stakeholders would never have invested in enabling the intellectual and computational platform needed for the capabilities they now highly value. SERC's investment was critical to creating these capabilities. The commitment of SERC's sponsors to supporting the fundamental research needed to address complex problems and issues in national security, healthcare delivery, higher education, and other important domains have been critical to providing the means and motivations to transform these systems.

1. What was the problem being addressed? Why was it hard and is it important?

- **Healthcare:** How can proven healthcare interventions be economically scaled to benefit large populations of patients?
- **Higher Education:** How can institutions of higher education address the tuition cost bubble in the US in light of challenging change scenarios?

2. What was new in the approach and why do we think it will be successful?

- Our models addressed these questions computationally, leveraging large, comprehensive health data sets, providing compelling interactive visualizations.
- Our models addressed these questions computationally, leveraging large, comprehensive education data sets, providing compelling interactive visualizations.

3. Who should care about this problem?

- Everyone is affected by these problems. They involve many trillions of dollars of annual expenditures. Beyond money, improved health and education affect everyone's lives. Society is better off because of these efforts.

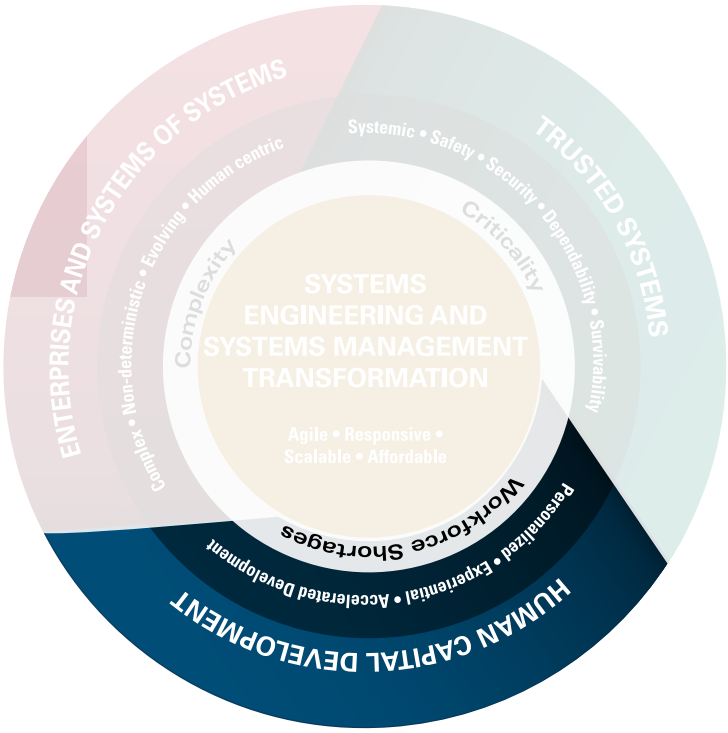
4. What are the risks and payoffs?

- The payoffs are immense and the risks are minimal. The key is providing compelling evidence to policy makers, key executives, important stakeholders, and people in general that the delivery of health and education can be dramatically improved while also being economically affordable.

5. What difference will this research make?

- If we focus and execute, we can deliver on the promise to foster a healthy, educated, and productive population that is competitive in the global marketplace.

HUMAN CAPITAL DEVELOPMENT



Providing ways to ensure that the quality and quantity of systems engineers and technical leaders provide a competitive advantage for the DoD and defense industrial base. Research must determine the critical knowledge and skills that the DoD and IC workforce require as well as determine the best means to continually impart that knowledge and skills.

HCD Area Goal: *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.*

One paper and one research task in the HCD area are highlighted in this transition report:

- *Body of Knowledge and Curriculum to Advance Systems Engineering (BKCASE)*
- *Helix – Workforce Evolution 2018-2019 (RT-198/WRT 1004)*

RESEARCH COUNCIL MEMBERS FOCUSED ON THIS THEMATIC AREA:

Jon Wade

Chief Technology Officer, SERC; Associate Director for Academic Research, International Council on Systems Engineering (INCOSE); Systems and Software Division Director and Distinguished Research Professor, School of Systems and Enterprises, Stevens Institute of Technology

BODY OF KNOWLEDGE AND CURRICULUM TO ADVANCE SYSTEMS ENGINEERING (BKCASE)

Principal Investigator: ***Art Pyster***
University: ***Stevens Institute of Technology (formerly), currently George Mason University***
Project page: ***https://sercuarc.org/project/?id=44&collaborator=Body+Of+Knowledge+And+Curriculum+To+Advance+Systems+Engineering+%28BKCASE%29***

Body of Knowledge and Curriculum to Advance Systems Engineering (BKCASE)
Advancing the State of the Discipline

The term "systems engineering" originated in Bell Laboratories in the 1940s, though the activities of systems engineering predated this term. As an integrative multi-disciplinary approach, one of the critical challenges as systems engineering has matured as a discipline has been defining its scope and activities and their boundaries with other disciplines. Part of the identity crisis in systems engineering for many years was that while the body of literature about the discipline grew, there was no clear or consistent view on what the body of knowledge in the discipline really entailed. Likewise, though academic programs in systems engineering saw explosive growth in the 1990s and early 2000s, there was little commonality or consistency between these programs. Employers hiring academically trained systems engineers struggled to understand what skills and abilities they could expect from these graduates.

In 2009, the Body of Knowledge and Curriculum to Advance Systems Engineering (BKCASE) project was created to address these challenges through two primary products: the Guide to the Systems Engineering Body of Knowledge (SEBoK) and the Graduate Reference Curriculum for Systems Engineering (GRCSE). Establishing a body of knowledge for systems engineering had been attempted many times before, but through the SERC was finally successful. Led by Art Pyster (then Stevens) and David Olwell (then the Naval Postgraduate School (NPS)), BKCASE brought together over 70 authors from around the world to create a critical reference for the discipline of systems engineering. The BKCASE team built the SEBoK and GRCSE over three years, maturing not only the products themselves but, through engagements with multiple professional societies, the discipline itself. The SEBoK v. 1.0, released in September 2012, was the first body of knowledge in any field published not as a document but as a wiki, intended to evolve easily as the discipline matured. GRCSE was delivered in December 2015 and provided the first formalized, community-led guidance for systems engineering graduate curricula.

In 2013, the SERC transitioned the SEBoK and GRCSE to a Governing Board, moving these critical assets from research to an established community resource. INCOSE, the IEEE Computer Society, and the SERC still govern BKCASE today. The SEBoK is overseen by an Editor in Chief, with support from an Editorial Board and dozens of authors from around the globe.

The latest version of the SEBoK, v. 1.9.1, was published 16 October 2018 and is available at sebokwiki.org. Since publication, the SEBoK has had over 1.5 million visitors and a total of 3 million page views, making it one of the most widely-used resources for systems engineering in the world. New versions of the SEBoK are released roughly every six months, making it one of the most rapidly evolving bodies of knowledge known.

GRCSE was updated in 2015 and was used as a critical input for the Accrediting Board for Engineering and Technology (ABET) to develop evaluation criteria around systems engineering. GRCSE is currently under revision; updates will include GRCSE itself as well as new considerations for undergraduate engineering education around systems.

HELIX – WORKFORCE EVOLUTION 2018-2019

Principal Investigator: Nicole Hutchison
University: Stevens Institute of Technology
Sponsor: ODASD (SE) / OUSD (R&E)
Research Task: 198/WRT 1004
Project Page: https://sercuarc.org/project/?id=45&collaborator=Helix+%E2%80%93+Developing+Effective+Systems+Engineers

1. What was the problem being addressed? Why was it hard and is it important?

The Department of Defense has for years been concerned about the growth and development of its systems engineering workforce. A particular concern has been the anticipated retirement of senior systems engineers in the near future and an inadequate number of mid-level systems engineers to fulfill these positions. This resulted in the Helix project – which was initially developed to investigate what makes systems engineers effective. Previous Helix work included Atlas: The Theory of Effective Systems Engineers, an Atlas Implementation Guide, a Career Path Guidebook, and multiple publications.

The current task expands upon the research developed during the execution of earlier tasks supporting the Helix project. The main focus areas for Helix include

- Understand not just what makes individual systems engineers effective but also what constitutes an effective systems engineering capability for an organization.
- Investigate what factors beyond the systems engineering workforce influence systems engineering effectiveness.
- Utilize data mining techniques such as cluster analysis and natural language processing on the existing Helix dataset. The dataset – over 6000 pages of transcripts and notes from 363 individuals across 23 organizations – is large and complex. The Helix team previously had used qualitative data analysis to extract meaning and patterns from the dataset. While this has been largely successful – resulting in Atlas and implementation from a number of organizations – the manual approach is now too labor-intensive to maintain. Utilizing these techniques on the existing dataset will provide validation of the existing findings and will set the team up to more easily incorporate new data in future.
- Develop a model using the findings that reflects an organization's systems engineering effectiveness, and pilot this model with multiple organizations.
- Use the model to develop a simulator than an organization can utilize to "test" changes designed to impact organizational systems engineering capability.

2. What was new in the approach and why do we think it will be successful?

To date, the Helix project researchers had collected data from 486 people at 31 organizations. Atlas is mature enough for earlier adopters with limited help from the Helix team, and is documented in a way that enables others to understand the motivations, methodology, principles, architecture, and details of the theory. Early methods and tools to apply Atlas have been developed and piloted with a small set of early adopters to help grow their systems engineers.

Despite the progress made to date, additional work is required to ensure that Helix and Atlas can fulfill their potential impact within the community. The research questions that guide Helix today are:

i. How can organizations improve the effectiveness of their systems engineering workforce?

ii. How does the effectiveness of the systems engineering workforce impact the overall systems engineering capability of an organization?

iii. What critical factors, in additional to workforce effectiveness, are required to enable systems engineering capability? Five key research gaps were identified by SERC. The primary focus of the proposed Helix research will be to close these gaps and document them in a way that will enable others to adopt Atlas more readily. Further, Helix needs to be embraced and utilized by the overarching systems engineering community. The 2017 effort will include a strong focus on transition activities, including working with professional societies such as the International Council on Systems Engineering (INCOSE), the National Defense Industrial Association Systems Engineering Division (NDIA SED), and the Institute of Industrial and Systems Engineers (IISE) to endorse and recommend use of Atlas.

The Helix team has launched two surveys – one for systems engineers and one for their peers, managers, and leaders – and continues in-depth interviews with participating organizations. These surveys combine two widely-used tools relating to organizational culture and teaming – the Competing Values Framework and the Quality of Interaction Index – with insights specific to organizational approaches to systems engineering identified in Atlas. (Examples below.) The combination of these three data sources creates a rich and insightful picture of organizational systems engineering capability.

3. Who should care about this problem?

Any organizations concerned with growth, development, and effectiveness of their systems engineers or who want to develop products of increasing complexity will find useful principles in Atlas. Individual systems engineers will also find guidance that they can use to assess and guide their own development. Organizations can use the findings of the organizational study to examine themselves with respect to what enables or impedes systems engineering implementation.

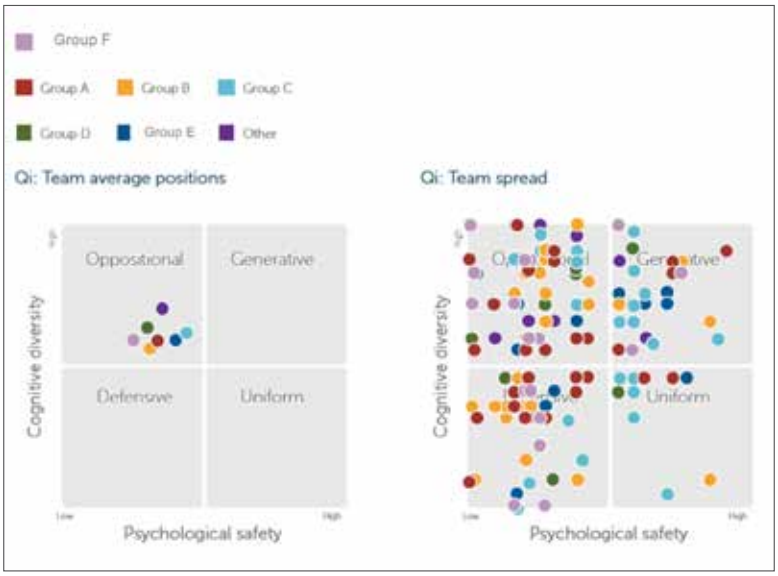
4. What are the risks and payoffs?

The primary risk in the research itself is that the dataset may not be varied enough or detailed enough to provide a representative sample of the systems engineering community and, therefore, conclusions generated may not be generalizable. The Helix team has intentionally increased organizational variety in its sample to help mitigate this risk.

A payoff, however, has been proven with the customization of Atlas at MITRE. There has been significant positive feedback on the guidance and clarity the tools provides on growing the individuals within their organization, and thus growing their workforce. The Helix team is aware of six organizations that have utilized Atlas to assess or improve their own workforce development efforts for systems engineers.

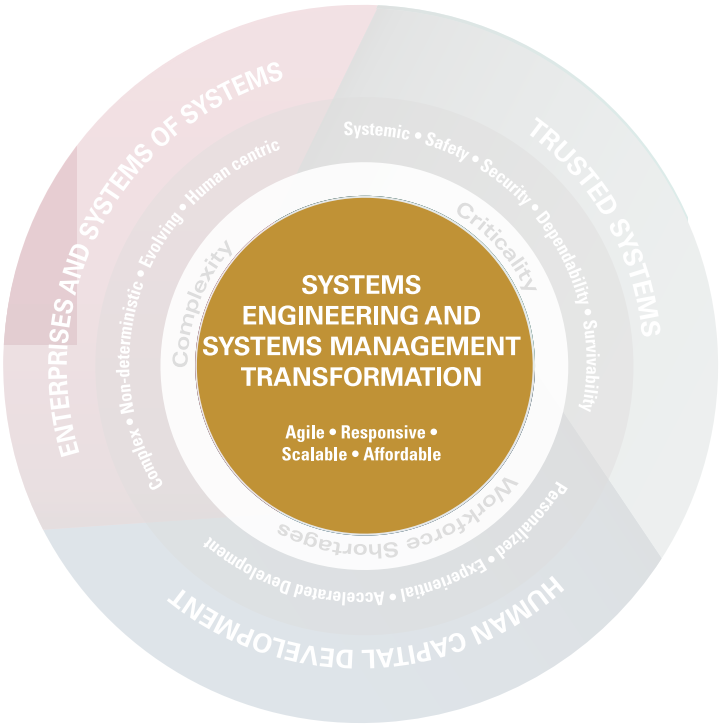
5. What difference will this research make?

Helix has already created tools that help individuals and organizations understand what can make systems engineers effective and foster intentional the growth and development of systems engineers. These tools have been adopted as part of the International Council on Systems Engineering (INCOSE) Professional Development Portal. Organizations which deem systems engineering as a critical capability for their goals will be able to utilize the Helix tools and findings to objectively assess their current capabilities, determine areas for potential improvements, and test these improvements using simulations before investing time and resources into them.



Comparison of team culture across different departments in a single organization.

SYSTEMS ENGINEERING AND SYSTEMS MANAGEMENT TRANSFORMATION



Providing ways to acquire complex systems with rapidly changing requirements and technology, which are being deployed into evolving legacy environments. Decision-making capabilities to manage these systems are critical in order to determine how and when to apply different strategies and approaches, and how enduring architectures may be used to allow an agile response. Research must leverage the capabilities of computation, visualization, and communication so that systems engineering and management can respond quickly and agilely to ensure acquisition of the most effective systems.

Goal: *Prototype, demonstrate, and provide methods to continuously advance the transformation of systems engineering to dynamic processes that leverage rapidly evolving 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.*

Six research tasks in the SEMT area are highlighted in this transition report:

- *Systems Engineering Business and Analytics (RT-213)*
- *Framework for Analyzing Versioning and Technical Debt (RT-193)*
- *Transforming Systems Engineering through Model-centric Engineering - Phase 5 (RT-195)*
- *Systems Engineering Approaches for Interagency Situational Awareness (RT-200)*
- *Formal Methods in resilient Systems Design using a Flexible Contract Approach - Part 2 (RT-210)*
- *Meshing Capability and Threat-based Science & Technology (S&T) Resource Allocation (RT-203)*

RESEARCH COUNCIL MEMBERS FOCUSED ON THIS THEMATIC AREA:

Barry Boehm

Research Council Chair and Chief Scientist Emeritus, SERC; TRW Professor of Software Engineering, Computer Science Department, University of Southern California; Director, USC Center for Systems and Software Engineering

Mark R. Blackburn

Senior Research Scientist, Stevens Institute of Technology

Paul Collopy

Professor, Industrial and Systems Engineering and Engineering Management, University of Alabama in Huntsville

SYSTEMS ENGINEERING BUSINESS AND ANALYTICS

Principal Investigator: K.P. Subbalakshmi
University: Stevens Institute of Technology
Sponsor: US ARMY RDECOM-ARDEC & ODASD(SE)
Research Task: 213
Project Page: https://sercuarc.org/project/?id=84&collaborator=Systems+Engineering+Business+and+Analytics

1. What was the problem being addressed? Why was it hard and is it important?

Practitioners and researchers abilities to access and utilize the "systems literature" is limited by the tens of millions of documents available, as well as the time they have available for compiling and digesting this evidence.

2. What was new in the approach and why do we think it will be successful?

The Systems Research Portal (SRP) provides electronic access to this immense literature organized into four topical areas (see Appendix):

- Systems Science
- Systems Engineering
- Operations Research
- Software Engineering

SRP provides capabilities for content aggregation, text analytics, and machine learning. SRP can "read" documents for users and provide highlight tailored to the specific elements of the queries posed by users.

3. Who should care about this problem?

Everyone who believes in the importance of evidence-based systems design and operations should embrace SRP. Humans cannot reasonably perform the tasks done by SRP.

4. What are the risks and payoffs?

We have built SRP and it will soon be deployed for evaluation. The main risk is lack of use due the cultural difficulties of engendering truly evidence-based decision making.

5. What difference will this research make?

The benefits of SRP include much better informed decisions, much less recreation of wheels, and an increasingly well-informed workforce.

ELEMENTS OF SYSTEMS RESEARCH PORTAL

SYSTEMS SCIENCE
- Complexity
- Prediction
- System State
  State Control
  State Estimation
- System Properties
  Networks
  Information
- Humans
  Decision Making
  Problem Solving
- Complex Adaptive Systems
- Systems of Systems

SYSTEMS ENGINEERING
- Requirements Analysis
  Analyze Missions & Environments
  Identify Functional Requirements
  Define Performance Requirements
  Define Design Constraints
- Functional Analysis & Allocation
  Decompose to Lower Level Functions
  Allocate Performance Requirements
  Define Functional Interfaces
  Define Functional Architecture
- Synthesis
  Functional Architecture è Physical Architecture
  Define Alternative System Concepts
  Select Preferred Product & Process
  Solutions
  Define Physical Interfaces

OPERATION RESEARCH
- System Design & Planning
  Planning and Strategy
  Technology Assessment and Adoption
  Allocation of Services and Technologies
  Location of Facilities
  Capacity Planning and Analysis
- Management of Operations
  Demand Forecasting
  Demand Management
  Service Scheduling
  Work Force Planning
  Work Force Scheduling
- Quality & Customer Satisfaction
  Quality Control
  Total Quality Management
  Six Sigma
  Quality Function Deployment
  Balanced Scorecard

SOFTWARE ENGINEERING
- Project Definition
- User Requirements Definition
- System Requirements Definition
- Analysis and Design
- System Build/Prototype/Pilot
- Implementation and Training
- Sustainment

FRAMEWORK FOR ANALYZING VERSIONING AND TECHNICAL DEBT

Principal Investigator: Ye Yang
University: Stevens Institute of Technology
Sponsor: RDECOM CERDEC
Research Task: 193
Project Page: https://sercuarc.org/project/?id=81&project=Framework+for+Analyzing+Versioning+and+Technical+Debt

1. What was the problem being addressed? Why was it hard and is it important?

COTS components are increasingly imposing long-term management issues such as obsolescence, poor reliability, lack of readiness, and inability to be readily maintaining systems in an efficient and effective manner. Most existing studies addressing COTS obsolescence issues have strong emphasis on the sustainment phases, with a focus on electrical components, namely in avionics and other complex military systems. The main challenge is the lack of a common metric and measurement framework to serve as basis for understanding, communicating, analyzing and predicting the life cycle consequences incurred by COTS obsolescence issues. Not having a view on both obsolescence risks and technical debts will cause system operators to make short-sighted decision that drive up the life cycle cost of a system. In order to achieve the expected economic benefits of COTS procurement, it is critical to enable program managers to better understand obsolescence cost before making informed COTS commitment decisions.

2. What was new in the approach and why do we think it will be successful?

In COTS-intensive CPS context, engineering decisions on acquiring quick COTS solutions would incur more "technical debt" to the user/customer organizations, which will need to be paid off in later maintenance or sustainment phases in the form of continuous upgrades. It is our belief that as Systems Engineering grows, esp. for COTS-based CPS systems, the need for a COTS-related technical debt analog grows. The RT-193 project adopted the notion of technical debt from the field of software engineering in order to provide a different perspective for coping with obsolescence problems in CPS system engineering life cycles. The project team conducted an intensive literature review and synthesized existing work on obsolescence management, and developed a taxonomy of COTS-related technical debts according to systematic signs discoverable during early COTS activities, which may contribute to obsolescence in later phases. These seven types of COTS technical debt include COTS functionality mismatch, performance mismatch, interoperability difficulty, versioning frequency, documentation and support readiness, and limitation on system evolution.

3. Who should care about this problem?

It is our intention to provide a unique technical debt perspective to facilitate the evaluation and reevaluation of defense acquisition programs which can better identify and mitigate COTS-related risks in the early acquisition phase, esp. obsolescence issues, among program managers, leadership, and other COTS-associated stakeholders.

4. What are the risks and payoffs?

The research direction is still in the early stages of developing automated, data driven, quantitative models and tools for identifying, analyzing, and managing technical debt for CPS. Major risks include: (1) the availability and quality of data sources associated with COTS technical debts; and (2) developing algorithmic, regression or machine learning based models for analyzing the impact of COTS TD. If applied in early acquisition, the payoff on avoiding unforeseen, expensive and unaffordable obsolescence issues could be substantial.

5. What difference will this research make?

The RT-193 project bridged the gap in existing obsolescence management studies and practices, which widely cover sustainment phase strategies such as life-time buys, last time buy, redesign, or substitution among other things, by introducing the notion of COTS technical debt and the associated taxonomy to be applied in the early acquisition phases of COTS-intensive CPS systems. It would be critical for CPS stakeholders to have the consistent language and analysis capabilities to maintain visibility of potential COTS obsolescence issues and costs so that they can make informed COTS commitment decisions.

TD Category	Description	Analogy to existing work
Function	The degree of functionality mismatch between COTS capabilities and system needs.	Local TD; Data TD
Performance	The degree of mismatches between COTS capabilities and system needs, w.r.t. performance properties.	MacGyver TD; Data TD
Interoperability	The degree of interface/ assumption mismatches among various interdependent COTS components, as well as among COTS and system custom components.	MacGyver TD; Data TD
Configuration Version	CPS configuration version planning needs to address solution availability plan. Greater tendency of COTS version upgrade/refresh may lead to more obsolete COTS.	Unavoidable TD; Local TD; MacGyver TD; Foundational TD; Data TD
Documentation & Support	Lack of documentation and vendor support will seriously impact on issue resolution related to obsolete COTS.	Unavoidable; Data TD
System Evolution Limitations	Requirements imposed by COTS may place great limitation on system evolution.	Unavoidable TD; Foundational TD; Data TD
Organic	People-centric perspective of TD focusing on organizational decision-making, behaviors, and practices associated with those personnel responsible for introductions of new technologies & systems and/or the sustainment of existing systems	Local TD; Naïve TD; Strategic TD

TRANSFORMING SYSTEMS ENGINEERING THROUGH MODEL-CENTRIC ENGINEERING - PHASE 5

Principal Investigator: Mark Blackburn
University: Stevens Institute of Technology
Sponsor: NAVAIR
Research Task: 195
Project Page: https://sercuarc.org/project/?id=26&collaborator=Transforming+Systems+Engineering+through+Model+Based+Systems+Engineering-NAVAIR

1. What was the problem being addressed? Why was it hard and is it important?

In 2013 the Naval Air Systems Command (NAVAIR) sponsored Systems Engineering Research Center (SERC) research to investigate the technical feasibility of a radical transformation through more advanced and holistic approaches to Model-Based Systems Engineering (MBSE); this was re-framed as Model Centric Engineering (MCE) as descriptive models, which replace documents are increasingly being integrated with computationally enable technologies that link and integrate discipline-specific and multi-physics models with descriptive models. MCE is now more broadly characterized as Digital Engineering (DE) as part of the Department of Defense (DoD) Digital Engineering Strategy. The traditional document-centric process at the beginning of the effort was based on rigorous Systems Engineering Technical Reviews in a traditional document-based acquisition process that was not allowing the deployment of warfighter capabilities to keep pace with the evolving threats by others around the world.

The NAVAIR challenge mandated an expected capability of MCE and more broadly DE that can enable mission and system-based analyses and engineering that reduces the typical time by at least 25 percent from what is achieved today for large-scale air vehicle systems. The need for increased speed for deploying warfighter capabilities extends beyond NAVAIR, and is needed more broadly across the DoD, where there are schedule delays, and also large cost overruns. The complexity of the DoD systems demands the use of technologies, methods, tools and transformed workforce practices that are used by leading industry organizations.

2. What was new in the approach and why do we think it will be successful?

The research started with a global scan of the most advance and holistic approaches to MCE/DE from 2013-2015. The aggregated information led NAVAIR leadership initiate the Systems Engineering Transformation (SET) in order to keep pace with organizations that are adopting and advancing MCE methods and technologies. NAVAIR looks to SET to transform, not simply evolve DE acquisition, in order to perform effective oversight of primes that are using modern modeling methods for mission and system engineer. NAVAIR leadership proposed a SET Framework to facilitate a new collaborative operational paradigm between government and industry fundamentally based on models to facilitate decision making about evidences of maturing designs.

NAVAIR applied an SE approach identifying six (6) Functional Areas, including SERC Research. The SERC Research team led the Surrogate Pilot Experiments starting in 2017 to characterize, assess and refine the SET Framework approach to Model-based Acquisition. Phase 1 of Surrogate Pilot experiments completed a deep dive in 2018 with mission, systems and a model for the Request for Proposal (RFP) Response from Surrogate Contractor for Surrogate Pilot experiments. The results demonstrated the art-of-the-possible doing “everything” in models using new operational paradigm between government and industry in an implementation of Collaborative Authoritative Source of Truth (AST). The surrogate contractor RFP response refined government mission and system models, and links detailed design and analysis information using multi-physics and discipline-specific models to descriptive system model with full traceability to mission requirements.

Unique to the approach provides a means for transforming traditional document-based Contract Data Requirement Lists (CDRLs) using Digital Signoffs for source selection technical evaluation directly in the RFP response model. Phase 1 results and models provide evidence and examples of unclassified models that are being used to create workforce development and training.

3. Who should care about this problem?

VADM Grosklags keynote at NDIA 2017 explained the issue of the US losing its military dominance. Elements of that keynote briefing have been presented at a number of public events. Every individual in the US should understand the potential of the threats. Our warfighters must be armed with the most advanced capabilities to protect the US citizens, and these warfighter capabilities need to advance in order for the US to maintain the dominance needed to maintain peace throughout our interconnected global societies.

4. What are the risks and payoffs?

The research summarized the broad expanse of MCE practices that are in use by the most advanced teams, and more actively in use by commercial organizations, because of the need to be competitive. However, because the government for years has used a document-centric approach to acquisition, there are challenges to transform the workforce, both on the government side and industry side, but there is also a need to deploy modeling capabilities for the government that are needed to support DE methods and practices.

There is also some misconception that if we simply arm the workforce with the modeling tools, that will be sufficient, but modeling methods are critical, as well as having the underlying computational capabilities, not just traditional Information Technologies (i.e., computers and network) in order to facilitate work do be performed in a collaborative authoritative source of truth in order to allow continuous asynchronous reviews to support decision making through inside and oversight of models of analysis and design. Traditional configuration management must be evolved to address model management and modulization to support large sets of cross-domain and multi-disciplinary teams to work collaboratively. While the surrogate pilot was able to provide demonstrations for many of these topics, the effort did not address cyber security of the underlying DE infrastructure, nor have they leveraged Artificial/Augmented Intelligence and Machine Learning technologies that are in use by leading commercial organization and being researched by some of the global threat nations.

The SET workforce efforts have brought on very skilled new hires that are fast in adopting and demonstrating expertise with modeling tools, but they need to use the appropriate modeling methods and be teamed with subject matter experts that have DoD relevant domain knowledge.

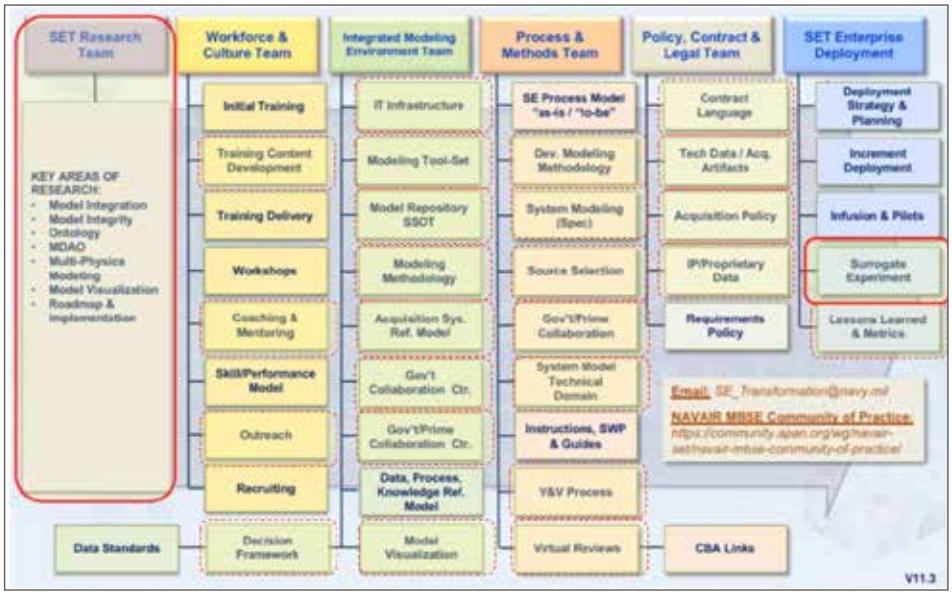
5. What difference will this research make?

This research has already made a difference, as facets of some of the demonstrated research are now being rolled out to other research projects and with some adoption by programs. The efforts provided inputs from our NAVAIR leadership that help to frame the DoD Digital Engineering Strategy, and as such our surrogate pilot experiments are providing some early demonstrations that align with the five (5) DE strategy goals. Our efforts seem to be influencing other research leading to DE Competency research and DE Policy efforts that are following our approach to "model everything" in order to demonstration the art-of-the-possible.

Figure 1 shows the six (6) major Functional Areas (and sub areas) of SET that includes:

- SET Research (conducted by the SERC)
- Integrated Modeling Environment
- Policy, Contracts and Legal
- Workforce & Culture
- Process & Methods
- SET Enterprise Deployment (and Surrogate Pilot Experiments)

While the two solid ovals represent the SET Research areas that are applied to the Surrogate Experiments, the research is also contributing to a wide array of sub areas (the dashed ovals).



SYSTEMS ENGINEERING APPROACHES FOR INTERAGENCY SITUATIONAL AWARENESS

Principal Investigator: Michael Orosz
University: University of Southern California
Sponsor: Space and Missile Systems Center (SMS)
Research Task: 200
Project Page: https://sercuarc.org/project/?id=70&collaborator=Systems+Engineering+Approaches+for+Interagency+Space+Situational+Awareness

1. What was the problem being addressed? Why was it hard and is it important?

While researchers have identified algorithms to improve space situational awareness through dynamic cross-cueing of different sensors, these approaches do not address the system engineering challenges of linking the tasking and data processing of multiple different sensors operated by different organizations under the authority of different chains of command. For example, a major challenge to overcome is that each agency typically relies on a different approach to scheduling, tasking and responding to events. A priority "one" in one agency may be a priority "zero" in another.

The Department of Defense and the Intelligence Community have established the NSDC as an interagency collaborative planning and tasking activity to operate across these organizations, but for the NSDC to be effective it will require systems engineering solutions to the interagency space situational awareness challenges.

This project undertook an initial analysis of system engineering approaches to implement data integration and exploitation as well as sensor tasking and cueing for next-generation space situational awareness sensors via the interagency National Space Defense Center (NSDC). The project provided the sponsor (SMC/SYAZ) with initial systems engineering research results to support of their Los Angeles-based team in recommending design and testing approaches for the Space-Based Space Surveillance Follow-On (SBSS FO) and other space superiority programs that are compatible with the Department of Defense's vision for the NSDC.

2. What was new in the approach and why do we think it will be successful?

The approach taken by USC/ISI was in getting interagency collaboration to support the project. Specifically, USC/ISI was able to undertake initial research into the appropriate requirements distribution and decomposition across the classes of sensor and processing systems that make up the interagency space situational awareness (SSA) architecture using the SBSS FO program as an exemplar. Based on this effort, an initial prototype effort was undertaken and recommendations for future demonstrations were compiled (all classified).

Although the project was terminated early (due to changes in sponsor priorities), USC/ISI was able to show the effectiveness of interagency collaboration within the Space Defense sector.

3. Who should care about this problem?

All Department of Defense acquisition programs where interagency collaboration is required to ensure system requirements are well understood.

4. What are the risks and payoffs?

The risks of undertaking this approach is that the overall project timeline may be delayed due to the time required to establish and maintain interagency collaborations. This delay includes the time required for team players to fully understand the differences in culture and processes that exist between multiple agencies. Complete understanding of all operations is required to ensure success of the project. The payoff, however, will be a multi-agency supported system that all agencies can leverage for greater operational efficiency. For example, capabilities that a single agency once solely supported will now be available to all agencies within the interagency solution.

5. What difference will this research make?

See above

FORMAL METHODS IN RESILIENT SYSTEMS DESIGN USING A FLEXIBLE CONTRACT APPROACH - PART 2

Principal Investigator: Azad Madni
University: University of Southern California
Sponsor: OUSD (R&E)
Research Task: 210
Project Page: https://sercuarc.org/project/?id=64&collaborator=Formal+Methods+in+Resilient+Systems+Design+using+a+Flexible+Contract+Approach

1. What was the problem being addressed? Why was it hard and is it important?

21st century DoD systems will continue to be complex, long-lived, likely to be adapted to new missions over their lifetime, and with stringent security requirements. These systems will need to be both safe and resilient when operating in uncertain environments subject to disruptions. Resilience requires flexibility, while safety requires the ability to prove correctness of the modeled system. This problem is hard because flexibility and correctness act in tradeoff fashion, and because the system has to operate in uncertain environments prone to disruptions. This problem is important because all DoD systems in the 21st century will require these characteristics to sustain performance for extended periods in increasingly more complex missions.

2. What was new in the approach and why do we think it will be successful?

For these types of 21st century systems, the system modeling approach needs to produce verifiable models while at the same time provide flexibility to adapt to changing conditions and learn from new observations. As important, the models should be able to provide useful outputs even with partial information. The new approach introduced the concept of a flexible contract, which we refer to as a resilience contract given our focus on system resilience. The resilience contract relaxes the assertions in a traditional contract to achieve the needed modeling flexibility and employs Partially Observable Markov Decision Process (POMDP) to handle uncertainty and enable in-use reinforcement learning. Figure 1 is a visual, graph-based representation of resilience contracts in a POMDP model.

3. Who should care about this problem?

The DoD has to address this problem for 21st century airborne, ground-based, and sea-based systems. This problem is of interest to aerospace and automotive companies for global supply chain management in the face of disruptions. This problem is also encountered with self-driving cars and their networks operating in poor visibility and with total or partial loss of communication.

4. What are the risks and payoffs?

The technical risk is the risk associated with all state-based representations such as POMDP which are susceptible to combinatorial explosion and are computationally intensive. Our approach ameliorates this risk by employing heuristic search that uses finite-step lookahead algorithm for computing POMDP. This approach is far less computationally intensive and does not require extensive prior information.

5. What difference will this research make?

This research will allow modeling of complex systems in which states are only partially observable and the system has to cope with and learn from systemic and external disruptions. For this class of problems, the model starts with incomplete information. Furthermore, the model adapts as needed when incoming information suggests that a different path would be preferable based on computation of belief probabilities. This approach has wide applicability in aerospace (e.g., multi-UAV planning and decision making in missions such as search and rescue) and automotive (e.g., probabilistic planning and decision-making during multi-UAV swarm operations). The research products are being transitioned to The Aerospace Corporation's MBSE team.

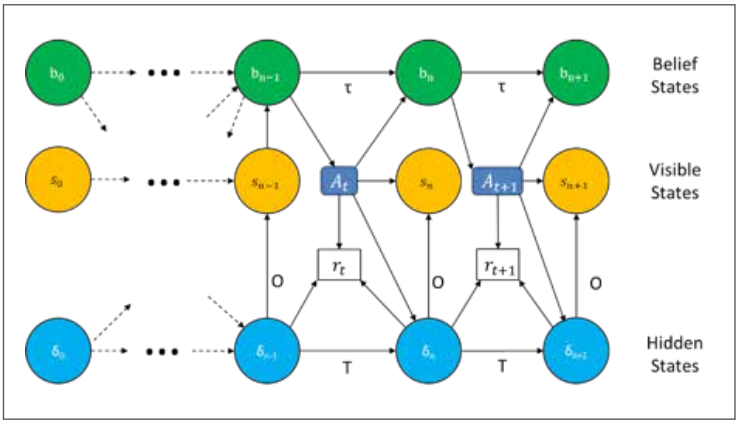


Figure 1- Resilience Contract Based on POMDP Modeling Approach

MESHING CAPABILITY AND THREAT-BASED SCIENCE & TECHNOLOGY (S&T) RESOURCE ALLOCATION

Principal Investigator: Carlo Lipizzi
University: Stevens Institute of Technology
Sponsor: US Army
Research Task: 203
Project Page: https://sercuarc.org/project/?id=61&collaborator=Meshing+Capability+and+Threat-based+Science+and+Technology+%28S%26T%29+Resource+Allocation

1. What was the problem being addressed? Why was it hard and is it important?

Capabilities-based planning attempts to break down traditional enterprise-level stovepipes during system development to stem the effects of a varied adversary. However, this approach tends to isolate the technical development community from strategic and tactical operational considerations. The technical communities charged with developing future weapons systems will be better informed by injecting relevant threat-based intelligence and operational scenarios into the capability-based planning approach. This approach has been piloted in late 2016 at the U.S. Army Combat Capabilities Development Command Armaments Center (CCDC AC) in the armament-systems domain. The researchers focused on creating a computational framework and a related system prototype that will:

- Replicate the aforementioned process developed at CCDC AC in 2016 to validate this notional computational architecture.
- Enhance the visualization and analytic capability to allow rapid, high fidelity decision making.
- Introduce additional parameters and variables to further refine the decision-making framework.

Being the source of information primarily text, creates two additional problems: extracting semantically relevant metrics from text and being able to work with text usable with no restriction by all the research team, but still representative of the target problem.

2. What was new in the approach and why do we think it will be successful?

We use our own algorithms and methods based on Natural Language Processing via Machine Learning techniques to transform text into sequences of context-sensitive numbers to be used to calculate metrics representing the different aspects of the problem and integrating them in an interactive visualization.

Because of the restrictions on the actual text from the Sponsor, we created a “proxy domain” semantically related to the real one. Working with the Sponsor, we selected the Private Security Industry as “proxy”. This gives the team access to unrestricted conspicuous sets of data/text.

In this research, two core systems, Technology Monitoring and Risk Panel systems, were designed and developed as agile, iterative prototypes with modular components. The modular components are vital building blocks that were designed to be used as components for the systems and the data collection process for the proxy domain.

3. Who should care about this problem?

Organizations that are interested in a text/data-driven approach to support decision-making can utilize the research findings from this project to address all what-if analyses, with a layer of Machine Learning trained by user interactions and suggesting “optimal” scenarios and allow users to monitor threats and emerging technologies involved in making and countering threats. The two main systems developed are:

Technology Monitoring System, a monitoring system to scan and detect technology data sources to provide insights and prepare for emerging technologies that may have an impact on the organization (please refer to the figure on the right for the Technology Monitoring System framework)

Risk Decision Support System, a text-based decision support system that collects information in real-time from text, analyze technological changes and organizations activities periodically, and recommend technology-driven scenarios (please refer to the figure on the right for the Risk Decision Support System framework).

4. What are the risks and payoffs?

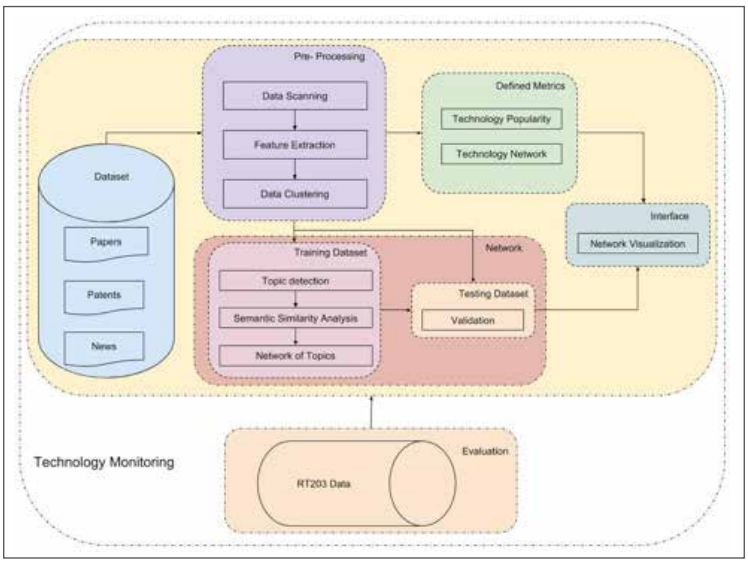
This research project is an applied research project, with deliverables that are not only reports but a useable, agile software prototype. That increases the complexity and introduces a high standard to be met in terms of code infrastructure and architecture. The team

is utilizing a combination of traditional Natural Language Processing and Machine Learning, extracting a numerical representation of texts, creating specific metrics for risk evaluation and for visualization. Most of the algorithms and methods used for the developments are either brand-new integrations of existing methods and algorithms or entirely new ones altogether. This adds a risk of having some of the algorithms being not as successful as expected, but also provides a competitive advantage when they succeed. Delivering a similar level of complexity in working prototypes is a task that logically requires a multi-year project.

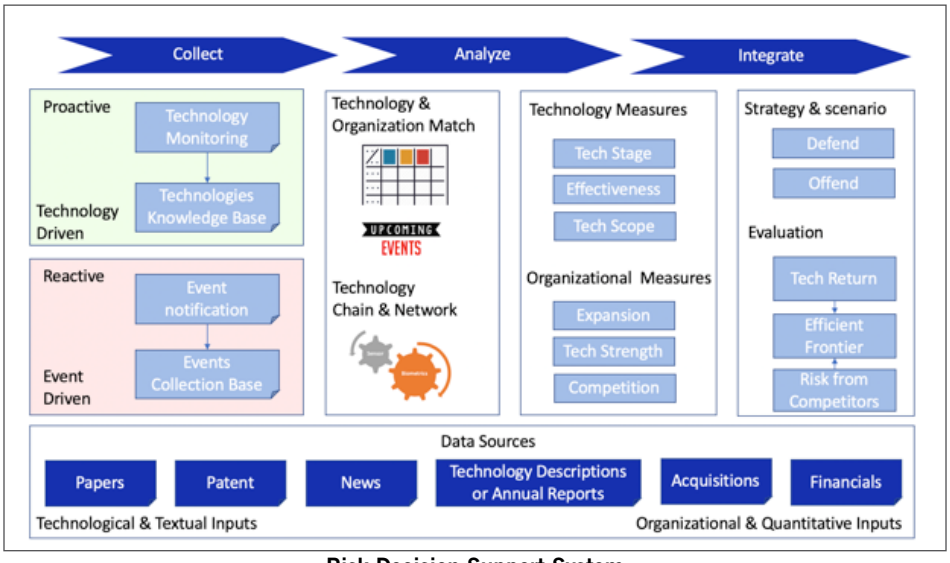
5. What difference will this research make?

The first difference this research is making is in providing a working prototype able to evaluate flexible risk scenarios from streams of text. The second is providing a radar screen for emerging technologies that is also taking into account possible future technologies and possible nonpublic technologies, by extrapolating past and present technology evolutions.

Besides the working prototypes, the research is breaking new grounds on contextual analysis and evaluation of streams of text for strategic decision making.

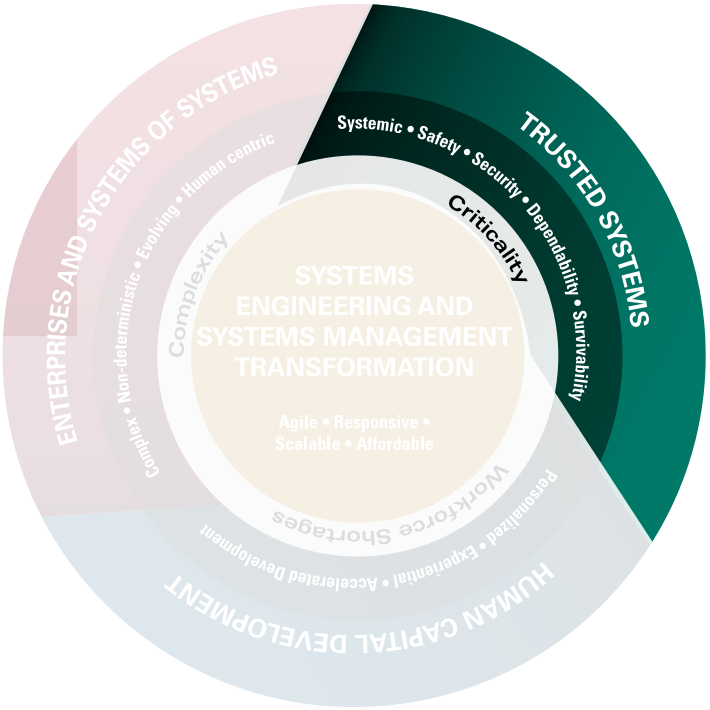


Technology Monitoring System



Risk Decision Support System

TRUSTED SYSTEMS



Providing ways to conceive, develop, deploy and sustain systems that are safe, secure, dependable, adaptable and survivable. Research must enable prediction, conception, design, integration, verification, evolution and management of these emergent properties of the system as a whole, recognizing these are not just properties of the individual components and that it is essential that the human element be considered.

TS Area Goal: *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. Five research tasks in the TS area are highlighted in this transition report:*

Four research tasks in the TS area are highlighted in this transition report:

- *Systemic Security and the Role of Heterarchical Design in Cyber-Physical Systems (RT-204)*
- *Security Engineering (RT-196)*
- *Identifying & Measuring Modularity Violations on Cyber-Physical Systems (RT-205)*
- *Game -theoretic Risk Assessment for Distributed Systems (GRADS) (RT-207)*

RESEARCH COUNCIL MEMBERS FOCUSED ON THIS THEMATIC AREA:

John M. Colombi

Associate Professor and Systems Engineering Program Chair, Air Force Institute of Technology (AFIT), Lt Col, USAF (Retired)

Barry Horowitz

Munster Professor of Systems and Information Engineering, University of Virginia

Valerie Sitterle

Principal Research Engineer and Chief Scientist, Systems Engineering Research Division, Electronic Systems Laboratory, Georgia Tech Research Institute (GTRI)

SYSTEMIC SECURITY AND THE ROLE OF HETERARCHICAL DESIGN IN CYBER-PHYSICAL SYSTEMS

Principal Investigator: Thomas McDermott
University: Stevens Institute of Technology
Sponsor: OUSD (R&E)
Research Task: 204
Project Page: https://sercuarc.org/project/?id=69&collaborator=Systemic+Security+and+the+Role+of+Heterarchical+Design+in+Cyber-Physical+Systems

1. What was the problem being addressed? Why was it hard and is it important?

This is Phase 1 of RT-204, which followed on from an incubator project of the same name. The goal underlying Systemic Security and the Role of Heterarchical Design in Cyber-Physical Systems (CPS) is to develop and gradually mature a capability to define and analyze security threats and counter-threat design patterns for cyber-physical systems. The envisioned approach aims to enable the greater community to rationally compare and select security implementations (a) in the early stages of design, 'designing in security,' and is (b) also applicable to already designed systems where security solution are needed.

2. What was new in the approach and why do we think it will be successful?

The research takes a holistic approach to integrating the CPS, attack vector(s), and security implementation(s) into a unified ecosystem model. The model is an abstraction of the greater system functional behavior, able to show how different types of failures may propagate through the system and what observable conditions these failures may manifest. The initial efforts focused on two concurrent lines of research: 1) methods to support generation of dynamic graph models from information extracted from existing MBSE formalisms, and 2) augmenting these structures with appropriate abstraction of functional characteristics (including from threats and protection patterns) and a means through which the dynamics associated with these structures and characteristics can be evaluated. The approach seeks to reveal in an automated toolset how well security design choices preserve critical system functionality necessary for mission success. A primary discovery revealed through the initial effort is need to look more deeply into how to model system functions in SysML so as to develop simulations of cyber-physical systems. Specifically, how should a functional architecture be defined in the form of an activity diagram that brings cyber and physical function types together with threat attack patterns in a meaningful and representative way and at what level of decomposition? Continuing work in the next phase will better position the research to answer the bidirectional problem of formal MBSE specification and simulation of the specified functional architecture. Additionally, future work will still need to mature the threat characterization and modeling space. This is a monumental gap in current understanding and practice. Work to date established that a functional model extracted from a formal system description, augmented with attack graphs, and a library of protective functional patterns, may provide an effective path toward earlier-stage design and analysis of security for cyber-physical systems. Further, the general approach developed in this work may serve as the basis for a repeatable, yet flexible approach. It is abstract enough to scale with increased model size, especially if the notion of a function library for CPS is established for community maturation. Dynamic simulation of an ecosystem view – comprised of the original (unprotected) cyber system, the threat functional capabilities and attack vectors revealing the critical cyber assets they will target – can provide insight concerning the health of the functional state space at a level of abstraction that should prove meaningful for design.

The effort also investigated how to capture notions of functional state for each functional element in a directed graph structure at appropriate levels of abstraction. The work evaluated ways to simulate the functional flow, using the functional state abstractions, to represent what behavioral dynamics could occur on the architecture. To make simulation of CPS functional graphs scalable, motifs – algorithmic expressions that represent functional states of each distinct functional class – are needed. This will make the assignment of different properties to different nodes in a graph scalable while still enabling variation that keeps the abstraction of functional flow representative of the system being modeled. The vision is that a library of functional element types will provide a customizable look-up from which different nodes may obtain class-appropriate motifs for functional state behavior. Through this approach, a directed graph derived from a system activity diagram may be specified in a table form, and each functional element auto-assigned representative expressions of functional state prior to simulation. The research developed a framework specifically for the purpose of analyzing how failure due to security risk (whether through degraded functionality, system compromise, or system corruption) could propagate through a functional architecture. Moreover, that framework should be extensible to the analysis of security protection pattern efficacy.

A tremendously significant consequence of the approach is that functional states may recover, not simply degrade, which reflects the resilience of the CPS. Initial graph simulation approaches were demonstrated on simple models, although significant future effort is required to simulate and test these types of simulation on complex systems of systems.

3. Who should care about this problem?

The The Strategic Technology Protection and Exploitation (STPE) division of OUSD/RE is leading DoD initiatives for Secure Cyber Resilient Engineering (SCRE) practices with a goal to better "design in security and resilience" for future system. They are the sponsor of this effort and expect to directly benefit. As the defense department and industrial base move more toward digital and model-based engineering, the viability of approaches to extract information from large models becomes more attractive. This is early research but should in the long-term lead to new classes of functional analysis methods the can automatically assess large complex systems at scale. As this research matures, it can be used to apply to models of any type of system, and can reflect system resilience beyond just security metrics. Modeling tool vendors are the eventual target market for the approach.

4. What are the risks and payoffs?

This effort established that a functional model extracted from a formal system description, augmented with attack graphs, and a library of protective functional patterns, may provide an effective path toward earlier-stage design and analysis of security for cyber-physical systems. Further, the general approach developed in this work may serve as the basis for a repeatable, yet flexible approach to predict security errors in system design. However, complex systems such as CPS ecosystems are not explicitly predictable, even when using first principles approaches. This effort is not trying to produce quantitatively accurate models in terms of expressing voltages, gains, inductances, etc. Rather the aim is to create functional abstractions of a system, using final node and edge states after graph simulation, that can accurately reveal whether critical system functions are preserved or not in the face of defined threats. Graphs offer a powerful approach through which system functional architectures may be captured and understood. As constructs, they do have limitations, however. For example, event-triggered flow and other forms of conditional iteration are not straightforward to represent using graph structures, even when using them to capture a functional level of abstraction. Such characteristics will likely require additional assumptions and/or adjustment to a resultant functional graph structure prior to dynamic evaluation. In addition, vertices (nodes) in these graphs represent functional elements, whether cyber or physical in nature, at the level of decomposition used by the system modeler. There is not yet a well-established foundation for what level of decomposition in the MBSE of functional architectures is most appropriate for cyber-physical systems. Example models explored by the research team do not contain sufficient functional information (represented in activity diagrams) to use this approach. Similarly, a system's behavior may have continuous, discrete, or even event-triggered interactions. These different concepts need to be better understood in terms of simulating system functionality at a level of abstraction that preserves relevance to the notion of security evaluation.

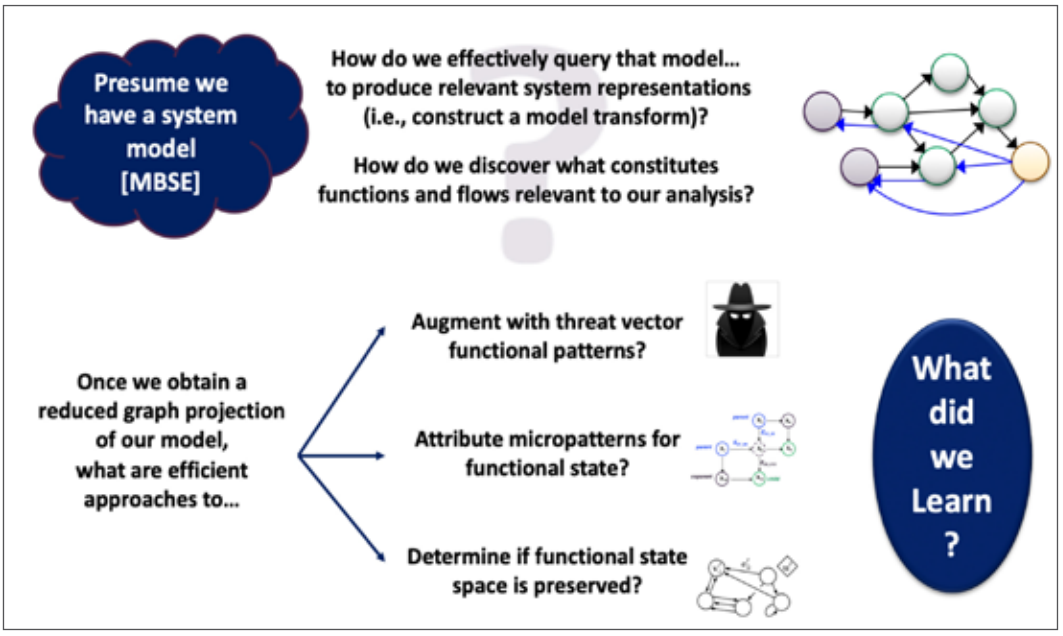
However, the aim of this work is an abstract depiction of dynamic behavior answering the question "Is the functional state space of the CPS system being modeled preserved or not under threat(s) and with designed security protection patterns in place?" This approach is flexible and will scale. The goal is not to produce a detailed, nearly first-principles model of the system. As such the approach should be quite useful to early stage requirements and architectural design activities. By leveraging patterns at the knowledge level, modelers can better understand how systems interact, and analysts can execute and analyze tradespace explorations in more effective, reproducible, and reusable ways.

5. What difference will this research make?

At this time, pretty much all security evaluation of CPS is done manually, or often not done. The state space explosion characteristic of all systems of any complexity prevents rigorous evaluation. This is an initial research activity that has the promise to automate security evaluation in early stages of design. Due to the increasing complexity created by the evolution of cyber-physical systems for Defense, new MBSE foundations, theories, and tools are needed to design, analyze, and verify these systems at various levels of abstraction. There are several benefits. First, methods of this type are necessary to deal with the existing complexity of most defense systems. Second, the approach holds promise of applying to full systems-of-systems, which are seldom fully evaluated. Third, the approach may prevent

security errors in design due to the target evaluation in early stage functional design. Through the efforts of this research, the power of a truly query-able system model has been described, which opens new opportunities for systems modeling and analysis. The research also revealed key gaps in current knowledge that, when addressed, will move the entire domain of design and security evaluation for cyber-physical systems forward in a meaningful way. The framework and foundations developed in this research to date are extensible to future maturation and use with different "truths", or views that comprise the MBSE process and practice. Together, they provide a path forward for simultaneous exploitation of MBSE, Digital Engineering, and Model-Based Design. Specifying an activity diagram view – a directed graph model of a functional architecture depicting functional elements and the resource, logical, or causal flow between them – as done in this work has tremendous implications for future practice. This approach may lead to a definition of best practices for transforming functional architectures into true, active analytical tools and not simply reference design templates.

Future cyber-physical systems will require hardware and software components that are highly dependable and reconfigurable. Trustworthiness will encompass preserving functionality when under attack and is consequently inseparable from security. Innovative approaches to abstraction and architectures may help unify the currently disparate subdisciplines within CPS research and development. In turn, this may enable more rapid and effective, modular design of these systems, create opportunities for different types of supportive analyses empowered by standardized abstraction methods, and even potentially spark innovative new design solutions.



High-Level Overview of RT-2014's Phase 1 Approach

SECURITY ENGINEERING

Principal Investigator: Peter Beling
University: University of Virginia
Sponsor: OUSD (R&E)
Research Task: 196
Project Page: https://sercuarc.org/project/?id=6&collaborator=Security+Engineering+%E2%80%93+Design+Patterns+and+Operational+Concepts

1. What was the problem being addressed? Why was it hard and is it important?

Security for Cyber-physical systems (CPS) refers to the application of defensive and resilience measures implemented to help sustain acceptable levels of operation in the face of adversarial actions. More specifically, defensive measures are the steps taken to prevent an adversary from disrupting, terminating, or taking over control of the operation of a system. Resilience, on the other hand, refers to the actions taken to ensure the continuity of the system's expected service in spite of adversarial actions. Methodologies and techniques for achieving enhanced system security in the cyber domain are prevalent and well-researched, and have been applied to CPS as well. However, the methods and techniques used for enhancing the security of strictly cyber systems are not sufficient for CPS due to their lack of focus and inability to account for the physical interactions inherent to CPS and the system's usage in a broader mission.

There is a need for new methodologies and associated sets of theory and tools to support preliminary design efforts for new cyber physical systems, with a timely and efficient process that addresses the cyber security requirements for the system. These methods should have the potential for increased scalability and traceability during design for cybersecurity of increasingly complicated, networked cyber–physical systems.

2. What was new in the approach and why do we think it will be successful?

This project developed two novel methodologies, Systems-Theoretic Resiliency Assessment Tool (STRAT) and Cyber Security Requirements Methodology (CSRM).

The CSRM is a methodology to develop cyber security requirements during the preliminary design phase for CPS. The methodology addresses the integration of both defense and resilience solutions and security-related software engineering solutions. CSRM identifies potential resiliency solutions based on the mission and system descriptions; inputs from stakeholders such as system operators, owners, and cyber-security experts; and the judgment of the systems engineering team.

To support CSRM, the Systems-Theoretic Resiliency Assessment Tools (STRAT) was developed. STRAT is composed of four main components: a formalized mission and system specification, a systems theoretic consequence analysis, model-based solution identification, and solution evaluation via dynamic simulation. STRAT injects into CSRM a more theoretical foundation for system behavior, causality models for accidents and mission losses, and traceability between vulnerabilities (or attacks) and mission degradation. STRAT builds on the systems-theoretic models and analysis tools developed by Leveson, such as the Systems Theoretic Accident Model and Process (STAMP) and Systems Theoretic Process Analysis (STPA), which have shown promise in aiding the generation of requirements and understanding the behavior of CPS with respect to safety and security. The overall flow of the methodology is illustrated in Figure 1.

This new approach was tested on a case study involving a hypothetical weapon system developed via CSRM. The results of CSRM alone, and CSRM with STRAT, are compared to assess the validity of the STRAT as a viable tool for identifying and recommending resilience solutions for a CPS. This work could be further expanded to also include cost analysis of resilience solutions and techniques for automating the model-based analysis.

3. Who should care about this problem?

This work is most relevant at the design phase for new systems or as part of a cybersecurity re-engineering of legacy systems. The methodology aims to engage mission/system owners, systems engineers, and cybersecurity specialists.

4. What are the risks and payoffs?

There are several challenges that we perceive in the preliminary design phase with respect to security of CPS. There are potentially

many important stakeholders with many different (valid) perspectives and knowledge bases. How does one use these stakeholders, and how are they organized? What should be done in terms of methodology, technology, and/or tools that can be used to make the process more scalable, traceable, and potentially repeatable? One thing that is clear is that there is not a single disciplinary collection that is capable of doing everything in terms of knowing how the system should behave, assessing the vulnerabilities or possible attacks to the system, or bringing to bear the operational characteristics in its intended environment(s)

5. What difference will this research make?

The major contribution of this work is a new methodology and associated set of theory and tools to support current preliminary design efforts for new cyber physical systems, with a timely and efficient process that addresses the cyber security requirements for the system. These methods have the potential for increased scalability and traceability during design for cybersecurity of increasingly complicated, networked cyber–physical systems. The findings of this study present similar results to a large-scale effort consisting of a team of systems engineers, operators, and cyber-security experts; however, the required time and manpower is significantly reduced, and the transparency and traceability in the information shared across these groups is improved. This allows experts to be used for confirming results rather than producing them, which can reduce project costs for expert time and increase expert productivity. The techniques presented in this work could allow for increased automation in security analysis, which would further increase the effectiveness and productivity of a traditionally labor-intensive process. A second contribution of this work is the creation of a common resilience management process that could be used in the development of new systems in multiple industries. Having such a methodology allows for earlier integration of operational test and evaluation in the design process as well as simplifying the design audit and review process.

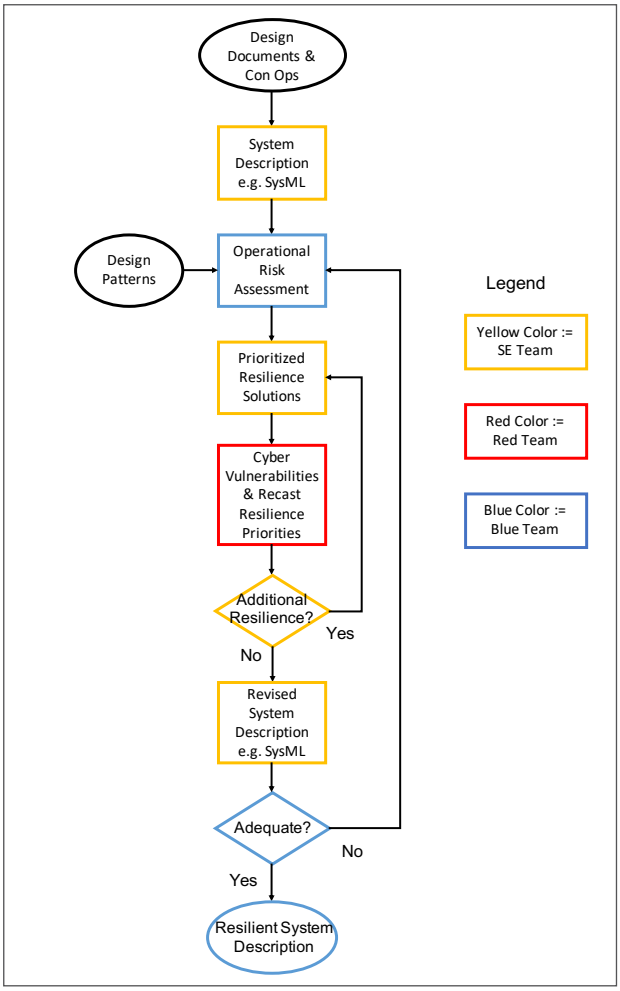


Figure 1

IDENTIFYING & MEASURING MODULARITY VIOLATIONS ON CYBER-PHYSICAL SYSTEMS

Principal Investigator: Lu Xiao
University: Stevens Institute of Technology
Sponsor: OUSD (R&E)
Research Task: 205
Project Page: https://sercuarc.org/project/?id=68&collaborator=Identifying+and+Measuring+Modularity+Violations+on+Cyber-Physical+Systems

1. What was the problem being addressed? Why was it hard and is it important?

The objective of this research is to develop techniques and metrics that would allow the Government to detect and measure modularity violations in developed and acquired cyber-physical systems. Recently, the Department of Defense has emphasized modular and open approaches to system development to improve interoperability, facilitate system evolution and technology insertion, and foster competition. Requirements such as the Modular Open Systems Approach (MOSA) have been imposed on acquisition efforts. However, it can be difficult for the Government to assess whether the resulting architectures and systems are truly modular. In short, there may be latent modularity violations that impede the realization of the benefits of modularity. This research will result in a set of objective metrics that could be used by Government program offices to evaluate contractor and collaborator compliance with modularity requirements.

Today, modularity in cyber-physical systems is evaluated in a subjective manner using assessment of the development environment and practices, checklists, inspection of design documents, etc. While such assessments are better than nothing, they are unable to detect latent modularity violations, as these are not apparent in design documentation. They may not even be detectable through formal methods as the violations may not be realized until the modules of the system are updated. Methodologies and tools have been built for analyzing modularity violations in software systems. Empirical studies have shown that modularity violations usually involve latent shared assumptions among source files that need to be better encapsulated in the modular design. However, the existing approach is limited in that it only addresses software systems implemented in a single programming language. Complex cyber-physical systems are composed of multiple heterogonous hardware and software sub-systems. Such systems are difficult to analyze because of data inconsistency and heterogeneity among the various sub-systems.

2. What was new in the approach and why do we think it will be successful?

To the best of our knowledge, an effective, general, and scalable approach to identify and measure modularity violations in cyber-physical systems does not exist. In RT-205, the research team from Stevens Institute of Technology leveraged two real-life cyber-physical systems, namely OpenWrt and MD PnP, as the study data sets to develop methods and metrics to help stakeholders identify and understand modularity violations in cyber-physical systems from different perspectives and levels of resolution. Toward that end, the team conducted three major research tasks:

- Task 1: Exploring alternative modular decompositions of a cyber-physical system. In this task, the team explored and compared different criteria to decompose a cyber-physical system into modules of different granularity based on separate stakeholder concerns.
- Task 2: Developing a Domain Concept Learner to Extract Hardware Related Concepts. In this task, the team leveraged natural language processing techniques to extract and understand hardware related concepts in cyber-physical systems. The team used the extracted concepts to identify and measure modularity violations involving hardware components.
- Task 3: Building decision framework demonstrator. In this task, the team built a proof-of-concept software demonstrator that combines the methodologies developed in the two prior tasks. The demonstrator shows how the developed methods and metrics can be applied to the two case study projects.

The demonstrator will contain three major components, as shown in Figure 1:

- Module Decomposer: This component takes the project data (e.g. configuration management systems and issue tracking database) and the user's decomposition strategy as an input to calculate a modular decomposition based on user's preferences.
- Domain Concept Leaner: Takes the hardware supporting documentation, such as wiki pages or design documents as input to learn the topic model of the domain hardware concepts.

- MV Analyzer: Leverages the calculated hardware concepts and the modular decomposition as input to identify potential Modularity Violations involving hardware and software components in a cyber-physical system. The stakeholder will see the potential modularity violations identified in their projects. This will enable them to be aware of potential modularity violations and understand the underlying hardware concepts that triggered changes to software modules. The goal is to help stakeholders to make informed decisions to maximize the benefits of modularization.

3. Who should care about this problem?

The output of this work would be immediately useful to DoD program offices that manage the development and acquisition of nominally modular systems. It would enable to them to quantitatively measure compliance with modularity requirements. Longer-term, it would also be relevant to other Government agencies and commercial firms as cyber-physical systems are becoming increasingly common.

4. What are the risks and payoffs?

Cyber-physical systems have wide-spread applications in different chapters of society. Thus, cyber-physical systems could be in very different problem domains. The analysis of modularity violations in different cyber-physical systems usually relies on relevant information from the domain. Therefore, the biggest risk is to build a general approach that works for different kinds of cyber-physical systems from different problem domains. The research team plan to test the developed approach on a broad spectrum of projects. If successful, it will provide valuable empirical experience of how modularity violations are caused in cyber-physical systems. It also helps to prevent vendor lock in, reduce the system maintenance costs, and increase the system competitiveness.

5. What difference will this research make?

In the long term, enforcing modularity requirements will assist the Government in avoiding vendor lock-in, which increases costs. Furthermore, it will enhance the Government's flexibility to independently upgrade and evolve the components of complex systems as the risk of triggering a latent modularity violation will be reduced.

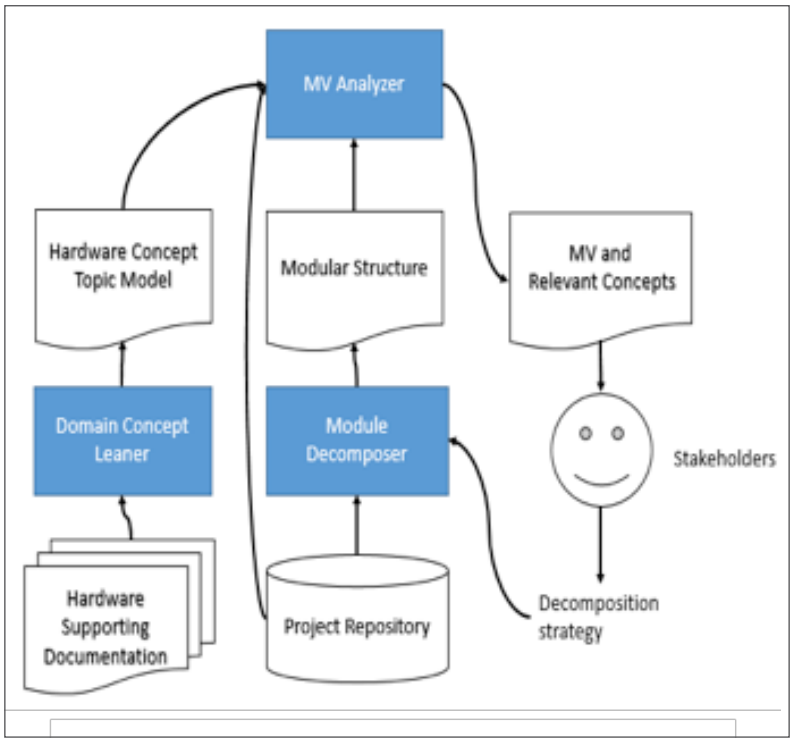


Figure 1- Proof-of-Concept Demonstrator

GAME -THEORETIC RISK ASSESSMENT FOR DISTRIBUTED SYSTEMS (GRADS)

Principal Investigator: Paul Grogan
University: Stevens Institute of Technology
Sponsor: ODASD (SE)
Research Task: 207
Project Page: https://sercuarc.org/project/?id=82&collaborator=Game-theoretic+Risk+Assessment+for+Distributed+Systems+%28GRADS%29

1. What was the problem being addressed? Why was it hard and is it important?

Collaborative system architectures across diverse application domains such as space systems and critical infrastructure can improve performance compared to independent alternatives by harnessing flexibility of phased deployment or joint operations, improving robustness through resilience to individual component failures, and increasing resource efficiency by matching available resources to localized demands. However, collaborative architectures also introduce new interdependencies between components and design actors which can lead to poor performance due to coordination failures, cascading failures, and loss of critical functions.

While systems engineering provides existing methods to understand and assess risk from systemic sources such as technical, programmatic, and environmental uncertainty, no existing methods indicate whether design actors should pursue a collaborative architecture or an independent one. Quantitative assessment of risks arising from collaboration seeks to mitigate or avoid fragile architectures susceptible to coordination failures, potentially saving significant resources from program overruns and cancellations attributed to poor alignment of values among partners. Addressing this problem requires modeling sources of value and interactive effects among independent design actors considering a collaborative architecture.

2. What was new in the approach and why do we think it will be successful?

GRADS transitions fundamental research from economics and game theory to systems engineering to quantitatively assess sources of risk in collaborative architectures. The "weighted average log measure of risk dominance" proposed by Nobel laureate Reinhard Selten quantifies normative strategy preferences in a class of multi-actor decision-making problems. It provides a relative measure of risk dominance that can compare alternative architectures and select one that manages both risk dominance and nominal performance. Coupled with a multi-actor value model to quantify actor preferences for alternative architectures, this metric has the potential to support conceptual phases of design by rapidly comparing and filtering architectures based on the relative stability under collaborative dynamics.

3. Who should care about this problem?

Multiple federal agencies including NASA, NOAA, and the DoD are currently pursuing collaborative space systems architectures with inter-agency, multi-nation, and public-private actors as a system of systems. Collaborative architectures introduce new interdependencies between and across agencies and firms with the goal of improving resource efficiency or technical performance. However, each design actor maintains an independent perspective on what drives individual value and the relative benefits of the joint (collaborative) versus an independent alternative. Pursing a collaborative architecture with poor strategic dynamics (measured via risk dominance) carries sources of collaborative risk, indicating the overall program is susceptible to coordination failures and cancellation.

Architecture selection using a quantitative basis such as the metric developed in GRADS allows each design actor to quantify preferences and measure relative tolerance to risk. Minor concessions to nominal performance through looser coupling between constituent systems may lead to significant reductions in risk and a higher chance of a successful joint program.

4. What are the risks and payoffs?

The fundamental idea behind risk dominance is rooted in theoretical economics and only addresses an abstract question of cooperative versus independent strategy selection. For application to engineering problems, the strategic-level analysis must be coupled with a

lower-level operational design analysis to select and evaluate architectural forms that align with alternative strategies. Furthermore, the economic theory uses several simplifying assumptions that do not reflect typical engineering problems. If these methods can be successfully adapted to systems engineering, the core theory provides a solid foundation on which to evaluate and assess collaborative architectures which is scalable to tradespace exploration and conceptual design studies.

5. What difference will this research make?

If incorporated in architectural design and selection activities, results from the GRADS project provide a quantitative basis on which to evaluate strategic dynamics present in system of system design problems and mitigate or avoid inherently risky collaborative architectures. Resulting architectures may become more conservative with respect to partner agencies or firms and rely on looser coupling between constituent systems, focusing on core functions or services that provide the most value. The main outcome seeks to avoid costly program overruns and cancellations due to poor strategic alignment among partner agencies and firms.

APPENDIX

RESEARCH TASKS INCLUDED IN THIS REPORT

Research Area	No.	Title	PI
ESOS		Healthcare	William Rouse
HCD		Body of Knowledge and Curriculum to Advance Systems Engineering (BKCASE)	Art Pyster
SEMT	193	Framework for Analyzing Versioning and Technical Debt	Ye Yang
SEMT	195	Transforming Systems Engineering Through Model-Centric Engineering - Phase 5	Mark Blackburn
TS	196	Security Engineering	Peter Beling
HCD	198	Helix - Workforce Evolution 2018-2019	Nicole Hutchison
SEMT	200	Systems Engineering Approaches for Interagency Situational Awareness	Michael Orosz
SEMT	203	Meshing Capability and Threat-based Science & Technology (S&T) Resource Allocation	Carlo Lipizzi
TS	204	Systemic Security and the Role of Heterarchical Design in Cyber-Physical Systems	Tom McDermott
TS	205	Identifying & Measuring Modularity Violations on Cyber-Physical Systems	Lu Xiao
TS	207	Game-Theoretic Risk Assessment for Distributed Systems (GRADS)	Paul Grogan
SEMT	210	Formal Methods in Resilient Systems Design Using a Flexible Contract Approach - Part 2	Azad Madni
SEMT	213	Systems Engineering Business and Analytics	K.P. Subbalakshmi

SYSTEMS ENGINEERING RESEARCH CENTER

University or Research Organization

1. Stevens Institute of Technology
2. University of Southern California
3. Air Force Institute of Technology
4. Auburn University
5. Carnegie Mellon University
6. Georgetown University
7. Georgia Institute of Technology
8. Massachusetts Institute of Technology
9. Missouri University of Science and Technology
10. Naval Postgraduate School
11. North Carolina Agricultural & Technical State University
12. Old Dominion University
13. Pennsylvania State University
14. Purdue University
15. Texas A&M University
16. University of Alabama in Huntsville
17. University of Maryland
18. University of Massachusetts Amherst
19. University of Virginia
20. University of South Florida
21. Virginia Tech
22. Wayne State University

SYSTEMS
ENGINEERING
RESEARCH CENTER

The SERC offices are located at

Stevens Institute of Technology
1 Castle Point on Hudson
Hoboken, NJ 07030

Phone: 201-216-8300

Email: SERC@SERCuarc.org

For more information about the SERC,
please visit the SERC website at

www.SERCuarc.org