# Systems Engineering Research Needs and Workforce Development Study – Pathfinder Study

SYSTEMS ENGINEERING RESEARCH CENTER

**Dinesh Verma, Ph.D.**

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

# SERC Core Competencies

Ability to conduct long-term, comprehensive SE research focused on DoD acquisition, including

- Enable integrated development and management
- New ways to link requirements to design
- Leverage modeling and simulation
- Link technical baselines to architectures
- Apply SE to acquisition of services

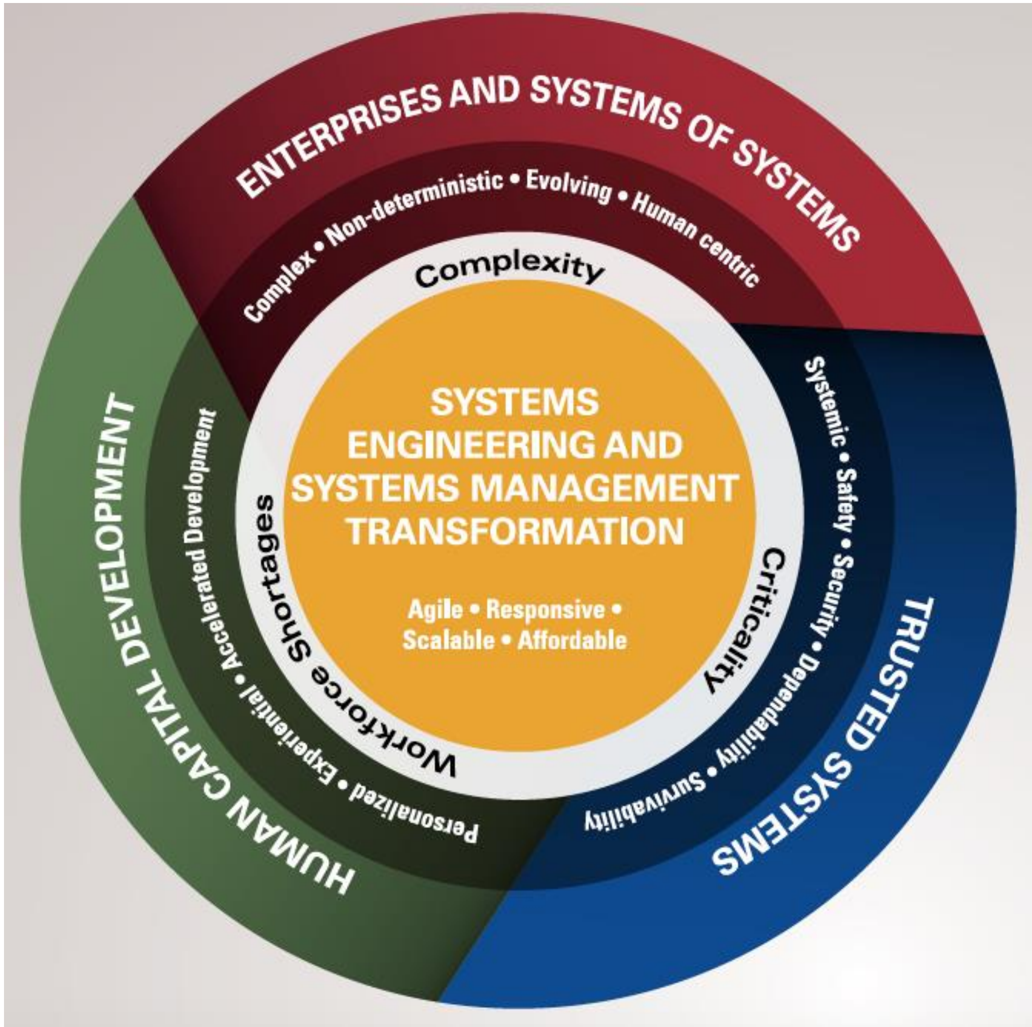
Ability to leverage developments in systems architecting, complex systems theory, systems thinking, systems science, knowledge management and SwE to perform research to advance the design and development of complex systems across all DoD domains, including

- System and open systems architecture/analysis
- SE in complex SoS and FoS environments
- Enterprise SE
- SW-unique extensions and modern SW-development technology
- Flexible SE environment
- Knowledge management
- Undergraduate/Graduate SE education needs

Ability to leverage developments in open systems standards, organizational theory, program management, SE management, and IT to provide needed integration of program/technical management MPTs, including

- Integrate TPMs with EVM
- Maturity reviews
- SE team structures, etc. for improvement
- Improved SE information sharing
- Rationale and way ahead for standards
- Toolsets throughout the life cycle
- Analyzing SE costs, accounts, and ROI
- SE metrics and leading indicators

# SERC Research Thematic Areas


ENTERPRISES AND SYSTEMS OF SYSTEMS
Complex • Non-deterministic • Evolving • Human centric
Complexity
TRUSTED SYSTEMS
Systemic • Safety • Security • Dependability • Survivability
Criticality
HUMAN CAPITAL DEVELOPMENT
Accelerated Development • Experiential • Personalized
Workforce Shortages
SYSTEMS ENGINEERING AND SYSTEMS MANAGEMENT TRANSFORMATION
Agile • Responsive • Scalable • Affordable

**Enterprises and SoS**

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

**Trusted Systems**

- *Systemic Security*
- *Systemic Assurance*

**Human Capital Development**

- *Evolving Body of Knowledge*
- *Experience Acceleration*
- *SE and Technical Leadership Education*

**SE & Systems Mgmt Transformation**

- *Affordability and Value in Systems*
- *Quantitative Risk*
- *Interactive Model-Centric Systems Engineering*
- *Agile Systems Engineering*

# Our Research Grand Challenges

**Enterprises and Systems of Systems**

Create the foundational SE principles and develop the appropriate MPTs to enable the DoD to architect, design, analyze, monitor and evolve complex enterprises and systems of systems to provide the DoD with an overwhelming competitive advantage over its current and future adversaries

**Trusted Systems**

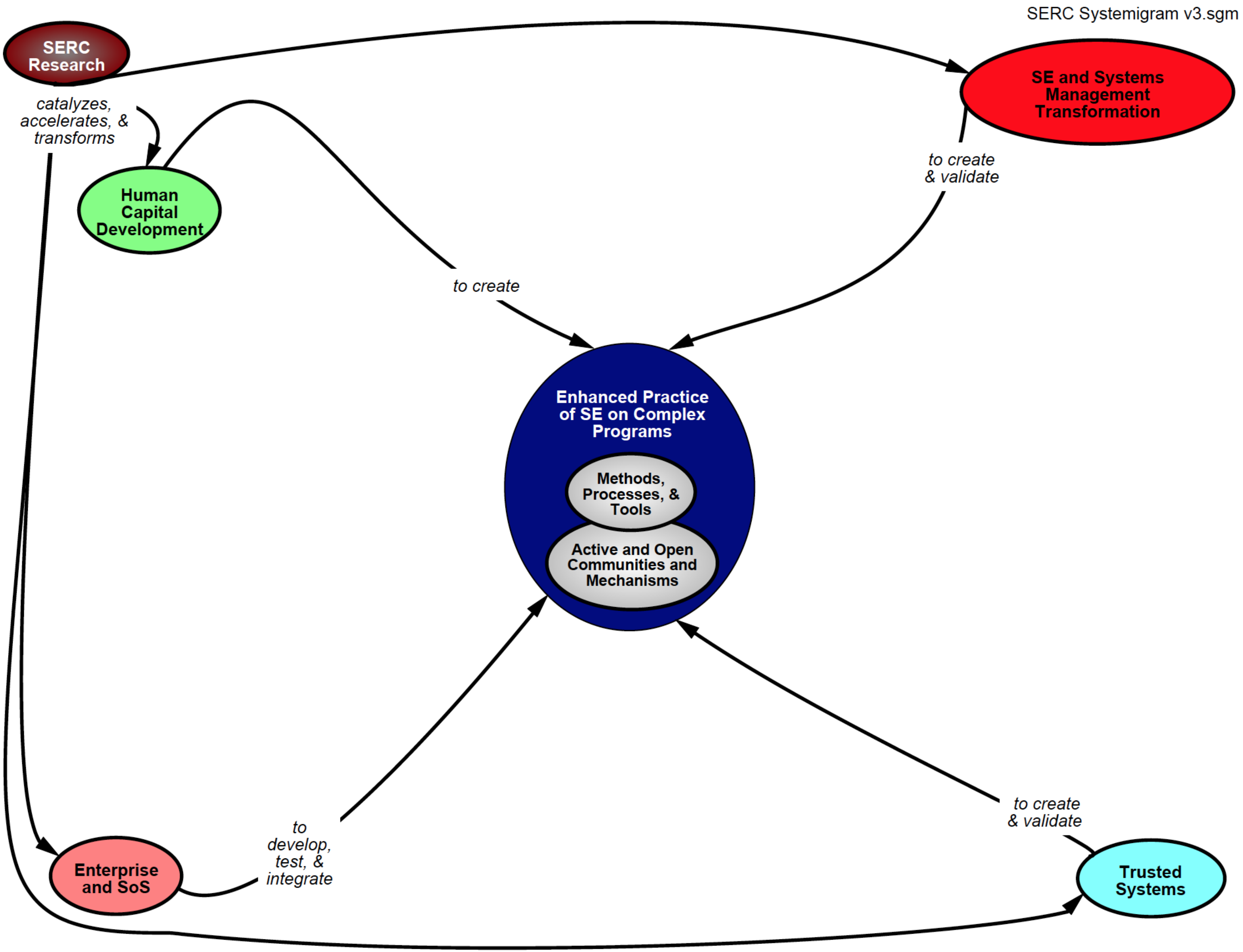
Achieve much higher levels of system trust by applying the systems approach to achieving system assurance and trust for the increasingly complex, dynamic, cyber-physical-human net-centric systems and systems of systems of the future

**SE and Systems Management Transformation**

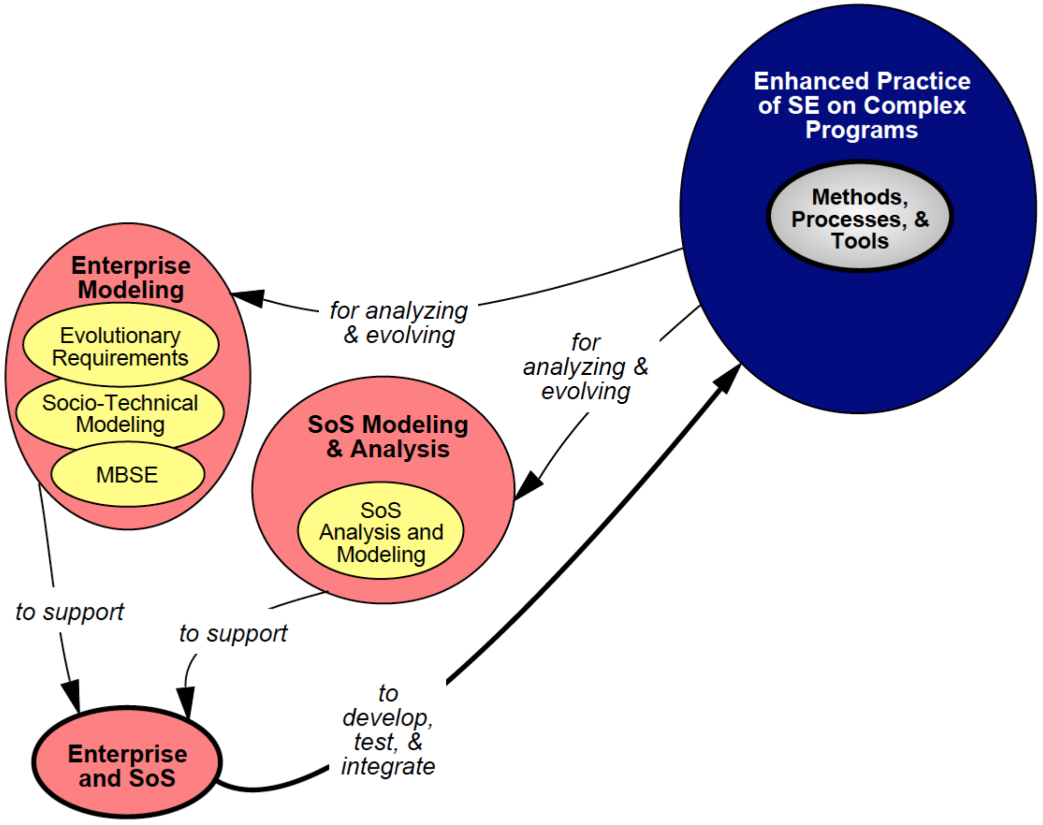
Transform the DoD community's systems engineering and management MPTs and practices to enable much more rapid, concurrent, flexible, scalable definition and analysis of the increasingly complex, dynamic, multi-stakeholder, cyber-physical-human DoD systems and systems of systems of the future

**Human Capital Development**

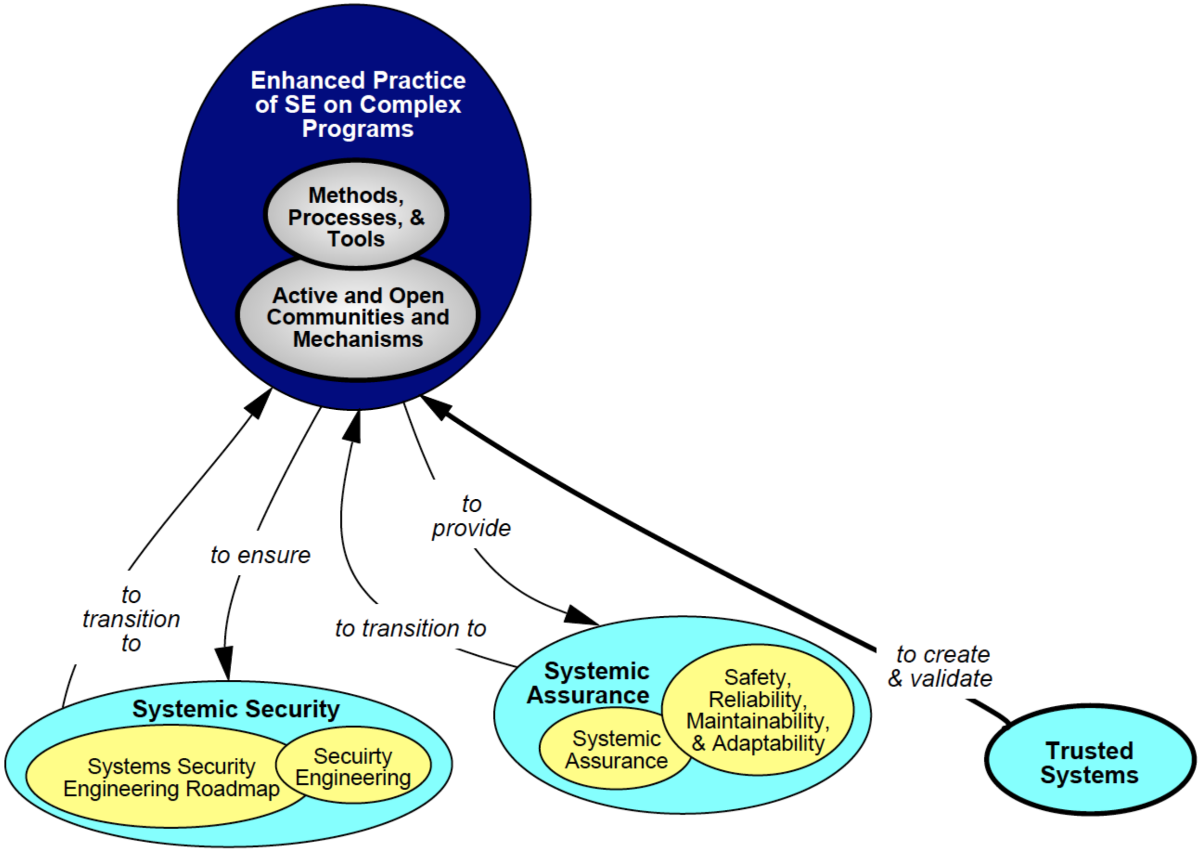
Discover how to dramatically accelerate the professional development of highly capable systems engineers and technical leaders in DoD and the defense industrial base and how to sustainably implement that discovery


SERC Systemigram v3.sgm
SERC Research
catalyzes, accelerates, & transforms
SE and Systems Management Transformation
Human Capital Development
to create
to create & validate
Enhanced Practice of SE on Complex Programs
Methods, Processes, & Tools
Active and Open Communities and Mechanisms
to develop, test, & integrate
to create & validate
Enterprise and SoS
Trusted Systems

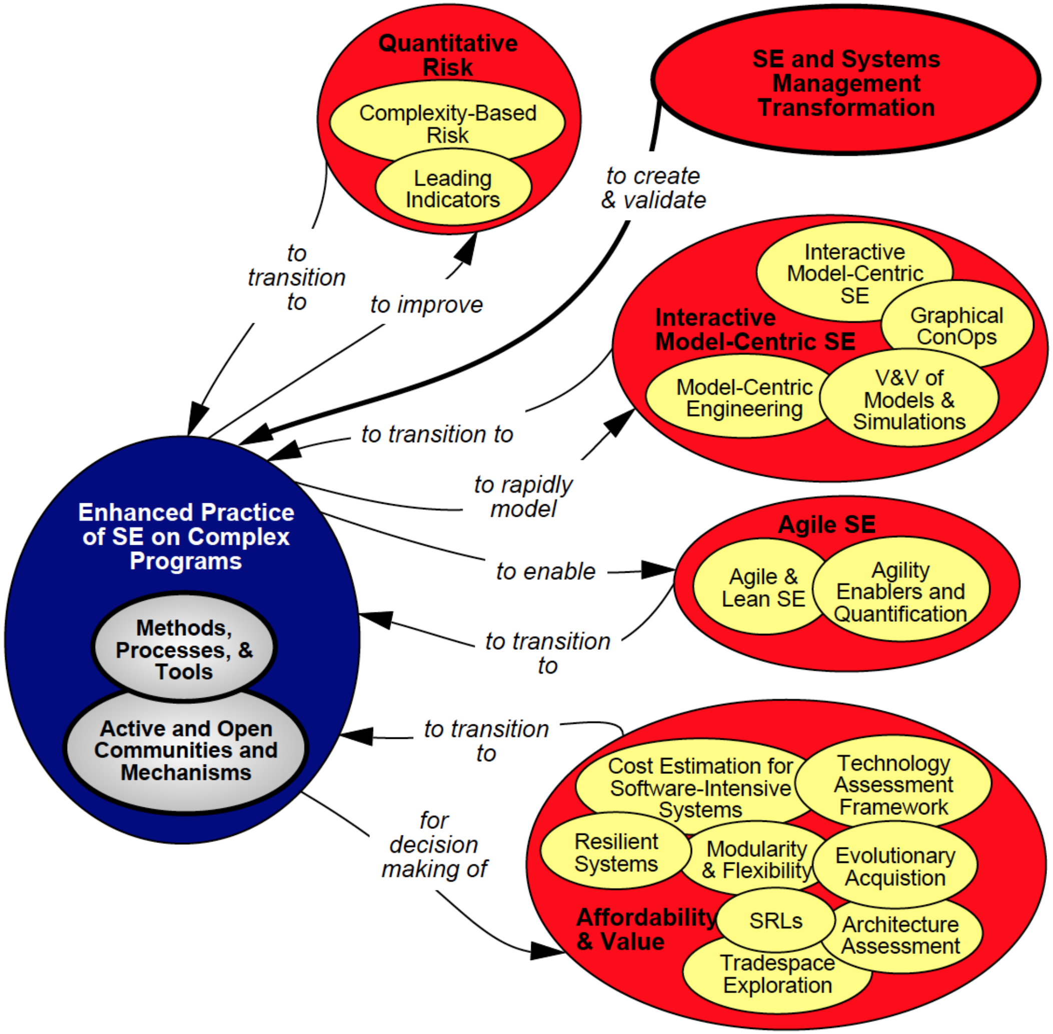
SERC Research



SERC Research


Enhanced Practice of SE on Complex Programs
Methods, Processes, & Tools
Active and Open Communities and Mechanisms
to transition to
to ensure
to transition to
to provide
to create & validate
Systemic Security
Systems Security Engineering Roadmap
Secuirty Engineering
Systemic Assurance
Systemic Assurance
Safety, Reliability, Maintainability, & Adaptability
Trusted Systems

SERC Research



Enhanced Practice of SE on Complex Programs

Methods, Processes, & Tools

Active and Open Communities and Mechanisms

Quantitative Risk

Complexity-Based Risk

Leading Indicators

to transition to

to improve

SE and Systems Management Transformation

to create & validate

Interactive Model-Centric SE

Interactive Model-Centric SE

Graphical ConOps

Model-Centric Engineering

V&V of Models & Simulations

to transition to

to rapidly model

Agile SE

Agile & Lean SE

Agility Enablers and Quantification

to enable

to transition to

Affordability & Value

Cost Estimation for Software-Intensive Systems

Technology Assessment Framework

Resilient Systems

Modularity & Flexibility

Evolutionary Acquistion

SRLs

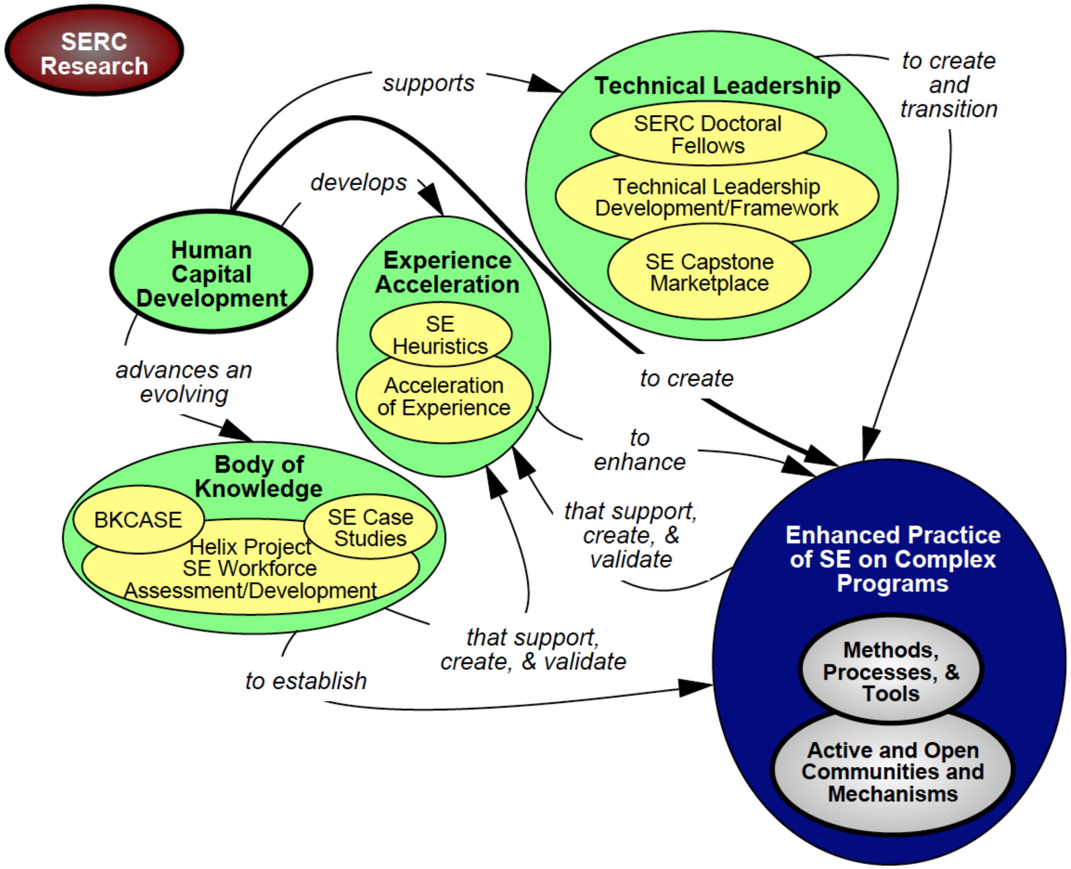
Architecture Assessment

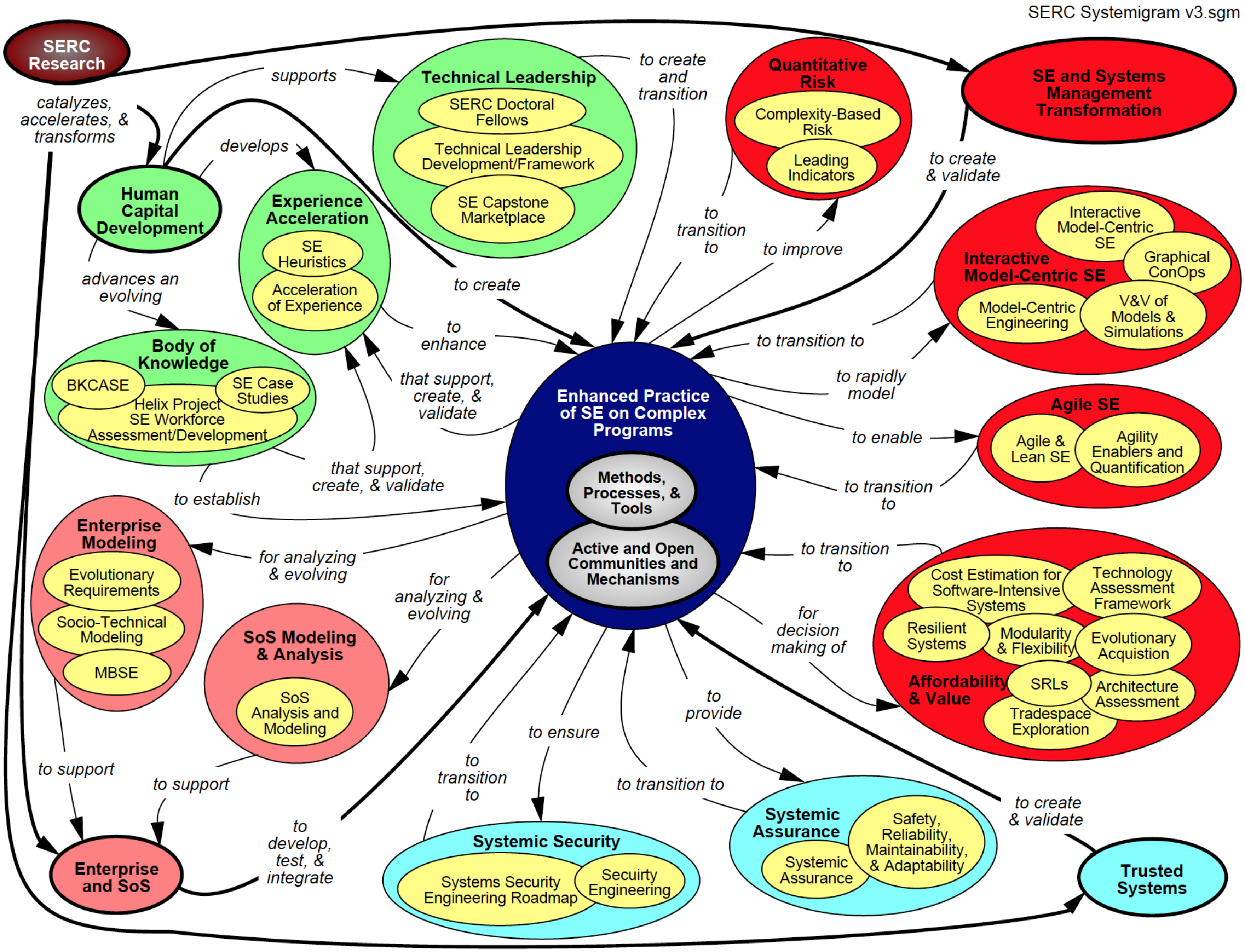
Tradespace Exploration

to transition to

for decision making of

SERC Systemigram v3.sgm

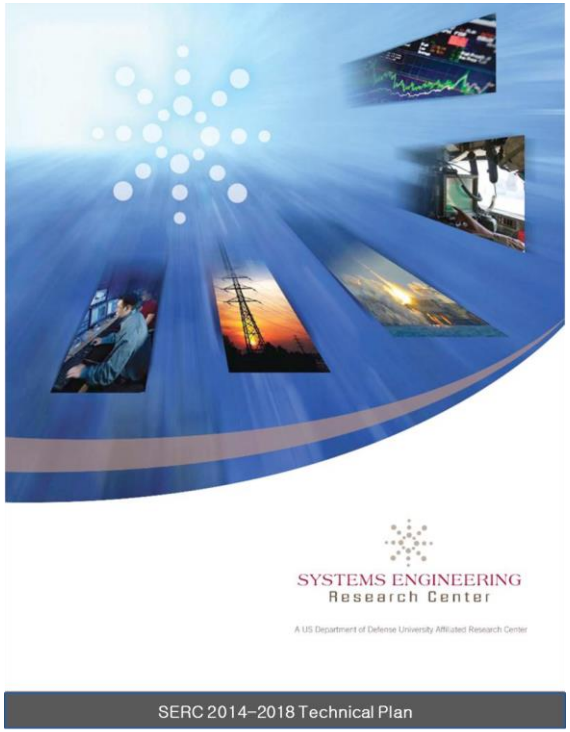

SERC Research
supports
Technical Leadership
SERC Doctoral Fellows
Technical Leadership Development/Framework
SE Capstone Marketplace
to create and transition
Human Capital Development
develops
Experience Acceleration
SE Heuristics
Acceleration of Experience
advances an evolving
to create
to enhance
Body of Knowledge
BKCASE
SE Case Studies
Helix Project
SE Workforce Assessment/Development
that support, create, & validate
that support, create, & validate
to establish
Enhanced Practice of SE on Complex Programs
Methods, Processes, & Tools
Active and Open Communities and Mechanisms


SERC Systemigram v3.sgm
SERC Research
catalyzes, accelerates, & transforms
supports
Technical Leadership
SERC Doctoral Fellows
Technical Leadership Development/Framework
SE Capstone Marketplace
to create and transition
Quantitative Risk
Complexity-Based Risk
Leading Indicators
SE and Systems Management Transformation
Human Capital Development
develops
Experience Acceleration
SE Heuristics
Acceleration of Experience
to create & validate
to transition to
to improve
to create
Interactive Model-Centric SE
Interactive Model-Centric SE
Graphical ConOps
Model-Centric Engineering
V&V of Models & Simulations
advances an evolving
Body of Knowledge
BKCASE
SE Case Studies
Helix Project SE Workforce Assessment/Development
to enhance
to transition to
that support, create, & validate
to rapidly model
Enhanced Practice of SE on Complex Programs
Methods, Processes, & Tools
Active and Open Communities and Mechanisms
Agile SE
Agile & Lean SE
Agility Enablers and Quantification
to enable
that support, create, & validate
to transition to
to establish
Enterprise Modeling
Evolutionary Requirements
Socio-Technical Modeling
MBSE
for analyzing & evolving
for analyzing & evolving
to transition to
Cost Estimation for Software-Intensive Systems
Technology Assessment Framework
Resilient Systems
Modularity & Flexibility
Evolutionary Acquistion
Affordability & Value
SRLs
Architecture Assessment
Tradespace Exploration
for decision making of
SoS Modeling & Analysis
SoS Analysis and Modeling
to ensure
to provide
to support
to support
to transition to
to transition to
to create & validate
to develop, test, & integrate
Enterprise and SoS
Systemic Security
Systems Security Engineering Roadmap
Secuirty Engineering
Systemic Assurance
Systemic Assurance
Safety, Reliability, Maintainability, & Adaptability
Trusted Systems

# SERC 2014-2018 Technical Plan

2014-2018 Technical Plan:

- Provided the vehicle by which to align the SERC Vision and Research Strategy with the Sponsor's Core funding priorities
- Described the SERC Vision, the Sponsor's needs, and the SERC's response to these needs
- Stated DoD's SE research *grand* challenges and how the SERC will apply core and other funding during 2014-2018 to address them
- Provided a multi-year roadmap of research programs to support this strategy.



SYSTEMS ENGINEERING Research Center

A US Department of Defense University Affiliated Research Center

SERC 2014–2018 Technical Plan

**We are in the process of developing our next five year Technical Plan**

# 2018-2023 SERC Technical Plan

- The foundation for the 2018-2023 SERC Technical plan to include:
  - General Framework: We retain the four research focus areas for continuity, but add missions that provide connections between these areas
    - "Missions" cut across the four thematic research areas
    - Mission areas might relate the following three imperatives:
      - **(Hard) Developing flexible designs that adapt, and are resilient to unknown missions and threats**
      - **(Wicked) Security: Safeguarding critical information, Designing systems resilient to a cyber adversary and other advanced threats and technologies**
      - **(Scary) Designing systems to take advantage of 3rd Offset Technologies, Engineering consideration for AI and Autonomy**
  - Critical Research: determination of critical research challenge areas to help realize the stated missions
  - Technical Plan 2018-2023: Currently under review by the EAB members

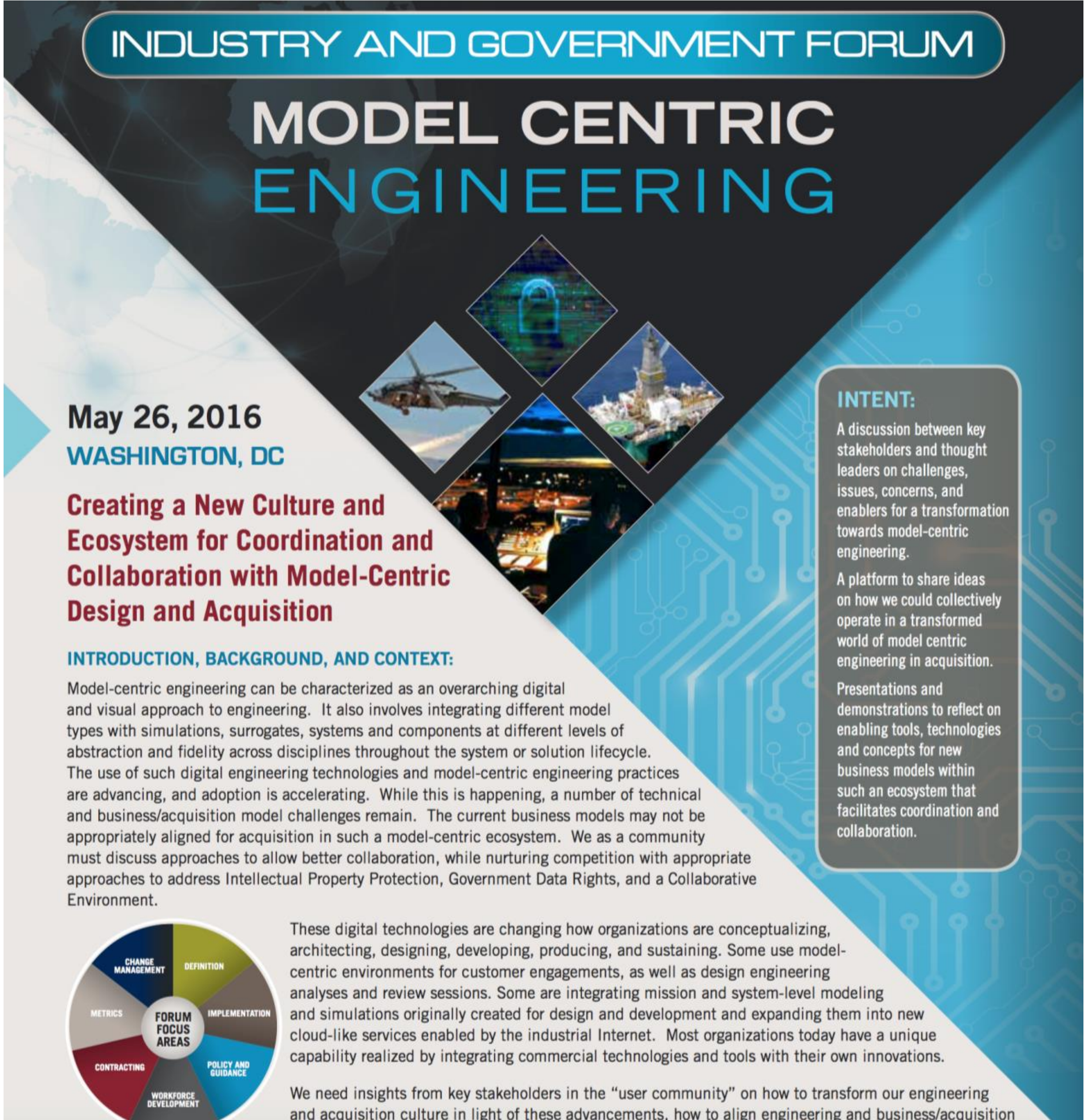
# Mission Areas

- **Hard – Velocity:** Developing and sustaining capabilities that support emergent and evolving mission objectives (deter and defeat emergent and evolving adversarial threats and exploit opportunities, affordably and with increased efficiency)
- **Wicked - Security**: Designing and sustaining the demonstrable ability to safeguard critical technologies and mission capabilities in the face of dynamic (cyber) adversaries
- **Scary - AI & Autonomy**: Developing and supporting system engineering MPTs to understand, exploit and accelerate the use of AI and autonomy in critical capabilities

**Significant community consent with these mission areas!**

## Research workshops that we held two years ago…

# Industry-Government Forum: Model Centric Engineering



INDUSTRY AND GOVERNMENT FORUM

## MODEL CENTRIC ENGINEERING

May 26, 2016

WASHINGTON, DC

### Creating a New Culture and Ecosystem for Coordination and Collaboration with Model-Centric Design and Acquisition

**INTENT:**

A discussion between key stakeholders and thought leaders on challenges, issues, concerns, and enablers for a transformation towards model-centric engineering.

A platform to share ideas on how we could collectively operate in a transformed world of model centric engineering in acquisition.

Presentations and demonstrations to reflect on enabling tools, technologies and concepts for new business models within such an ecosystem that facilitates coordination and collaboration.

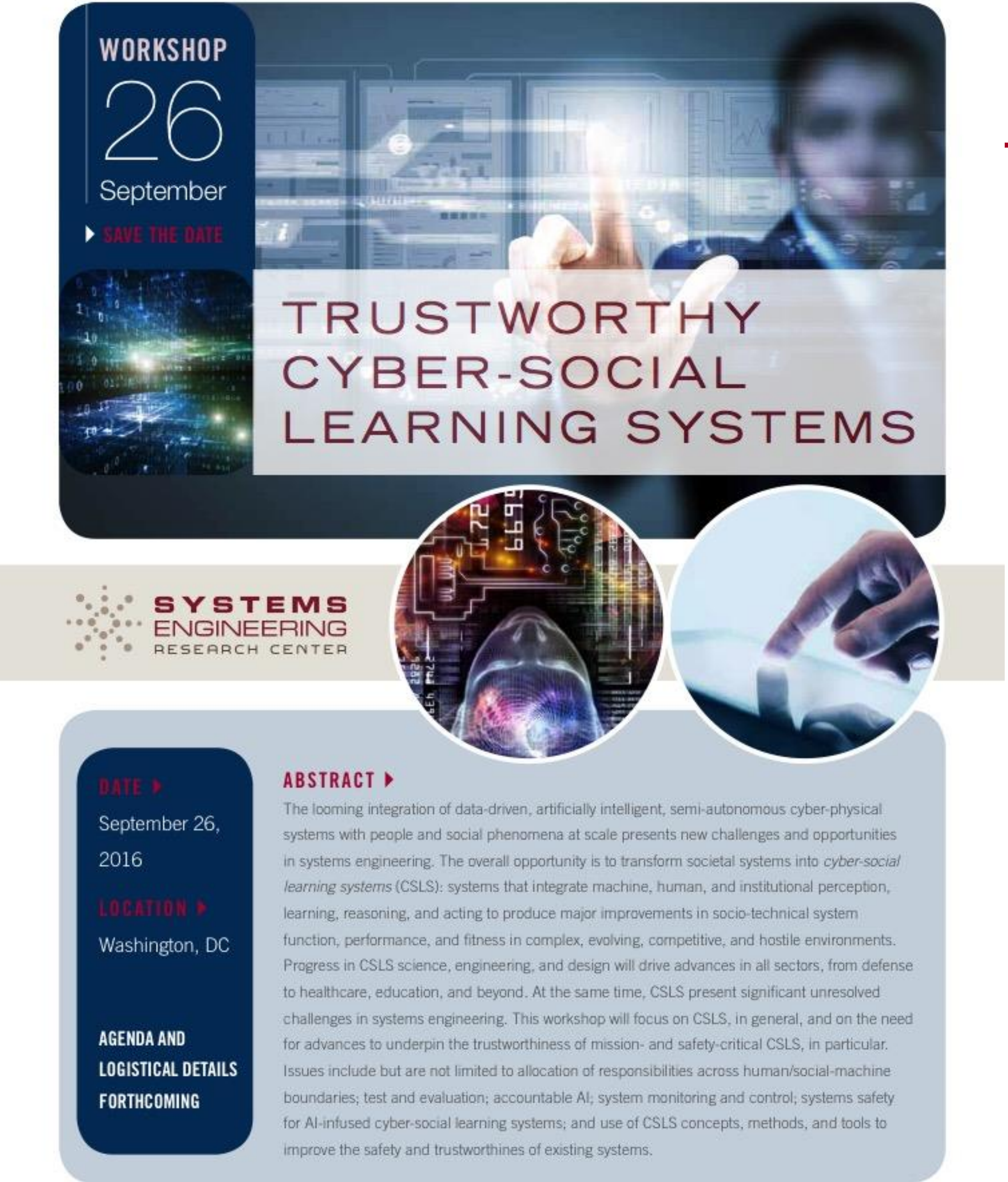
**INTRODUCTION, BACKGROUND, AND CONTEXT:**

Model-centric engineering can be characterized as an overarching digital and visual approach to engineering. It also involves integrating different model types with simulations, surrogates, systems and components at different levels of abstraction and fidelity across disciplines throughout the system or solution lifecycle. The use of such digital engineering technologies and model-centric engineering practices are advancing, and adoption is accelerating. While this is happening, a number of technical and business/acquisition model challenges remain. The current business models may not be appropriately aligned for acquisition in such a model-centric ecosystem. We as a community must discuss approaches to allow better collaboration, while nurturing competition with appropriate approaches to address Intellectual Property Protection, Government Data Rights, and a Collaborative Environment.

These digital technologies are changing how organizations are conceptualizing, architecting, designing, developing, producing, and sustaining. Some use model-centric environments for customer engagements, as well as design engineering analyses and review sessions. Some are integrating mission and system-level modeling and simulations originally created for design and development and expanding them into new cloud-like services enabled by the industrial Internet. Most organizations today have a unique capability realized by integrating commercial technologies and tools with their own innovations.

We need insights from key stakeholders in the "user community" on how to transform our engineering and acquisition culture in light of these advancements, how to align engineering and business/acquisition

**September 26, 2016; Invitation only attendance, limited to 35**



WORKSHOP

26

September

SAVE THE DATE

# TRUSTWORTHY CYBER-SOCIAL LEARNING SYSTEMS

SYSTEMS ENGINEERING RESEARCH CENTER

DATE

September 26, 2016

LOCATION

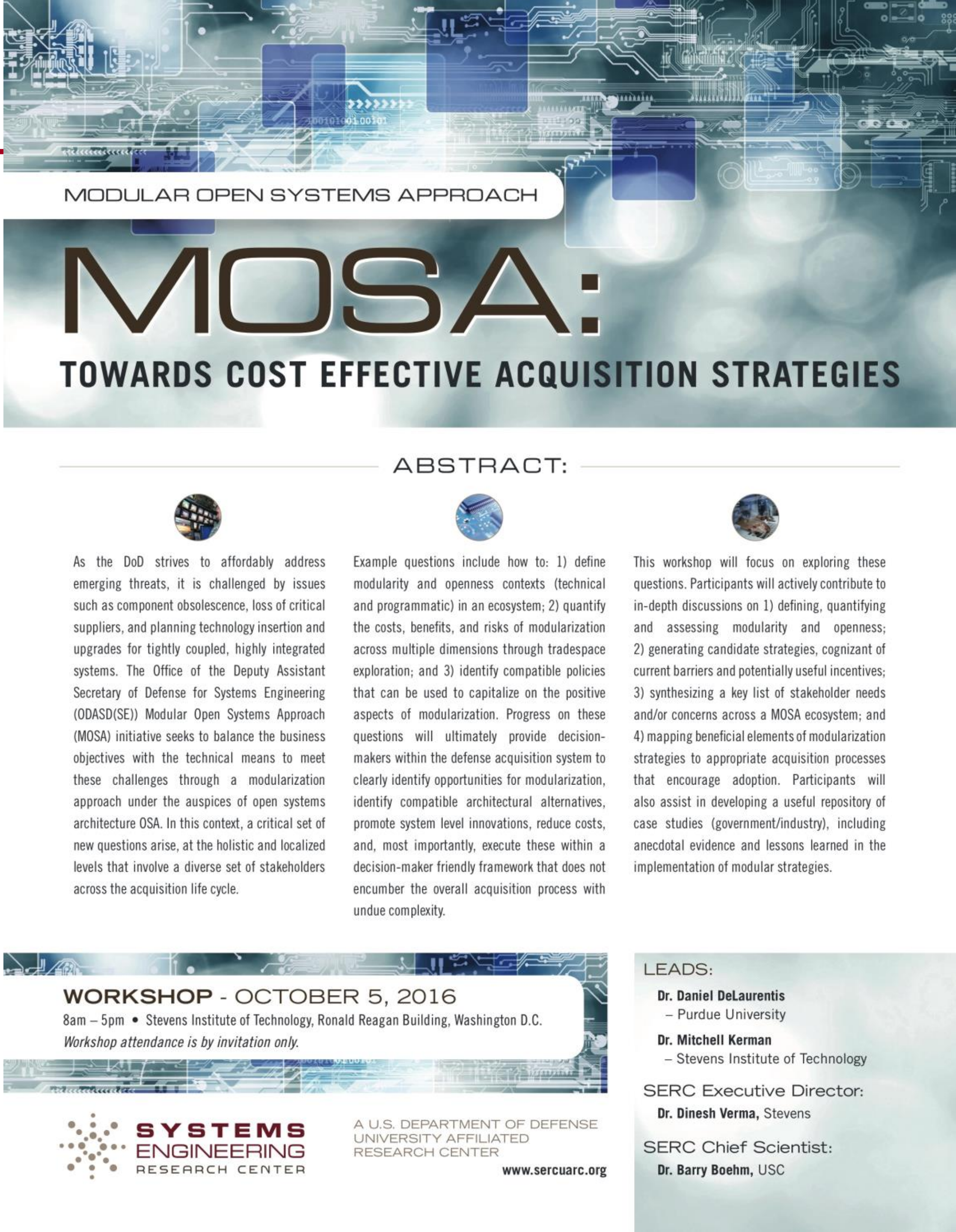
Washington, DC

AGENDA AND LOGISTICAL DETAILS FORTHCOMING

## ABSTRACT

The looming integration of data-driven, artificially intelligent, semi-autonomous cyber-physical systems with people and social phenomena at scale presents new challenges and opportunities in systems engineering. The overall opportunity is to transform societal systems into *cyber-social learning systems* (CSLS): systems that integrate machine, human, and institutional perception, learning, reasoning, and acting to produce major improvements in socio-technical system function, performance, and fitness in complex, evolving, competitive, and hostile environments. Progress in CSLS science, engineering, and design will drive advances in all sectors, from defense to healthcare, education, and beyond. At the same time, CSLS present significant unresolved challenges in systems engineering. This workshop will focus on CSLS, in general, and on the need for advances to underpin the trustworthiness of mission- and safety-critical CSLS, in particular. Issues include but are not limited to allocation of responsibilities across human/social-machine boundaries; test and evaluation; accountable AI; system monitoring and control; systems safety for AI-infused cyber-social learning systems; and use of CSLS concepts, methods, and tools to improve the safety and trustworthines of existing systems.

**October 5, 2016;**
**Invitation only attendance, limited to 35**



MODULAR OPEN SYSTEMS APPROACH

# MOSA:

## TOWARDS COST EFFECTIVE ACQUISITION STRATEGIES

### ABSTRACT:

As the DoD strives to affordably address emerging threats, it is challenged by issues such as component obsolescence, loss of critical suppliers, and planning technology insertion and upgrades for tightly coupled, highly integrated systems. The Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD(SE)) Modular Open Systems Approach (MOSA) initiative seeks to balance the business objectives with the technical means to meet these challenges through a modularization approach under the auspices of open systems architecture OSA. In this context, a critical set of new questions arise, at the holistic and localized levels that involve a diverse set of stakeholders across the acquisition life cycle.

Example questions include how to: 1) define modularity and openness contexts (technical and programmatic) in an ecosystem; 2) quantify the costs, benefits, and risks of modularization across multiple dimensions through tradespace exploration; and 3) identify compatible policies that can be used to capitalize on the positive aspects of modularization. Progress on these questions will ultimately provide decision-makers within the defense acquisition system to clearly identify opportunities for modularization, identify compatible architectural alternatives, promote system level innovations, reduce costs, and, most importantly, execute these within a decision-maker friendly framework that does not encumber the overall acquisition process with undue complexity.

This workshop will focus on exploring these questions. Participants will actively contribute to in-depth discussions on 1) defining, quantifying and assessing modularity and openness; 2) generating candidate strategies, cognizant of current barriers and potentially useful incentives; 3) synthesizing a key list of stakeholder needs and/or concerns across a MOSA ecosystem; and 4) mapping beneficial elements of modularization strategies to appropriate acquisition processes that encourage adoption. Participants will also assist in developing a useful repository of case studies (government/industry), including anecdotal evidence and lessons learned in the implementation of modular strategies.

**WORKSHOP** - OCTOBER 5, 2016

8am – 5pm • Stevens Institute of Technology, Ronald Reagan Building, Washington D.C.

*Workshop attendance is by invitation only.*

SYSTEMS ENGINEERING RESEARCH CENTER

A U.S. DEPARTMENT OF DEFENSE
UNIVERSITY AFFILIATED
RESEARCH CENTER

**www.sercuarc.org**

LEADS:

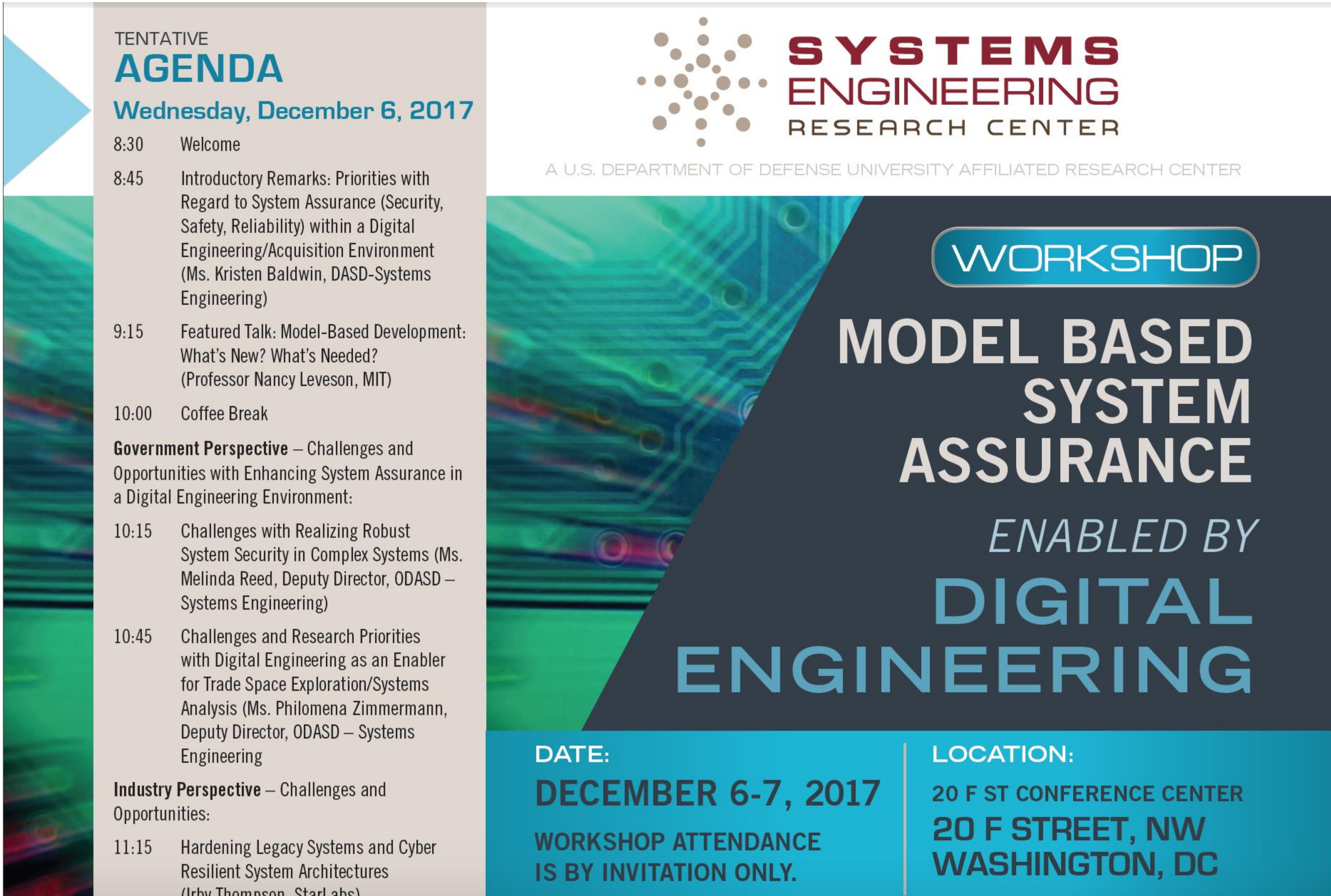
**Dr. Daniel DeLaurentis**
– Purdue University

**Dr. Mitchell Kerman**
– Stevens Institute of Technology

SERC Executive Director:
**Dr. Dinesh Verma,** Stevens

SERC Chief Scientist:
**Dr. Barry Boehm,** USC

# Research workshops that we held last year…



TENTATIVE

## AGENDA

### Wednesday, December 6, 2017

8:30 Welcome

8:45 Introductory Remarks: Priorities with Regard to System Assurance (Security, Safety, Reliability) within a Digital Engineering/Acquisition Environment (Ms. Kristen Baldwin, DASD-Systems Engineering)

9:15 Featured Talk: Model-Based Development: What's New? What's Needed? (Professor Nancy Leveson, MIT)

10:00 Coffee Break

**Government Perspective** – Challenges and Opportunities with Enhancing System Assurance in a Digital Engineering Environment:

10:15 Challenges with Realizing Robust System Security in Complex Systems (Ms. Melinda Reed, Deputy Director, ODASD – Systems Engineering)

10:45 Challenges and Research Priorities with Digital Engineering as an Enabler for Trade Space Exploration/Systems Analysis (Ms. Philomena Zimmermann, Deputy Director, ODASD – Systems Engineering

**Industry Perspective** – Challenges and Opportunities:

11:15 Hardening Legacy Systems and Cyber Resilient System Architectures (Irby Thompson, StarLabs)

SYSTEMS ENGINEERING RESEARCH CENTER

A U.S. DEPARTMENT OF DEFENSE UNIVERSITY AFFILIATED RESEARCH CENTER

WORKSHOP

# MODEL BASED SYSTEM ASSURANCE

*ENABLED BY*

# DIGITAL ENGINEERING

**DATE:**

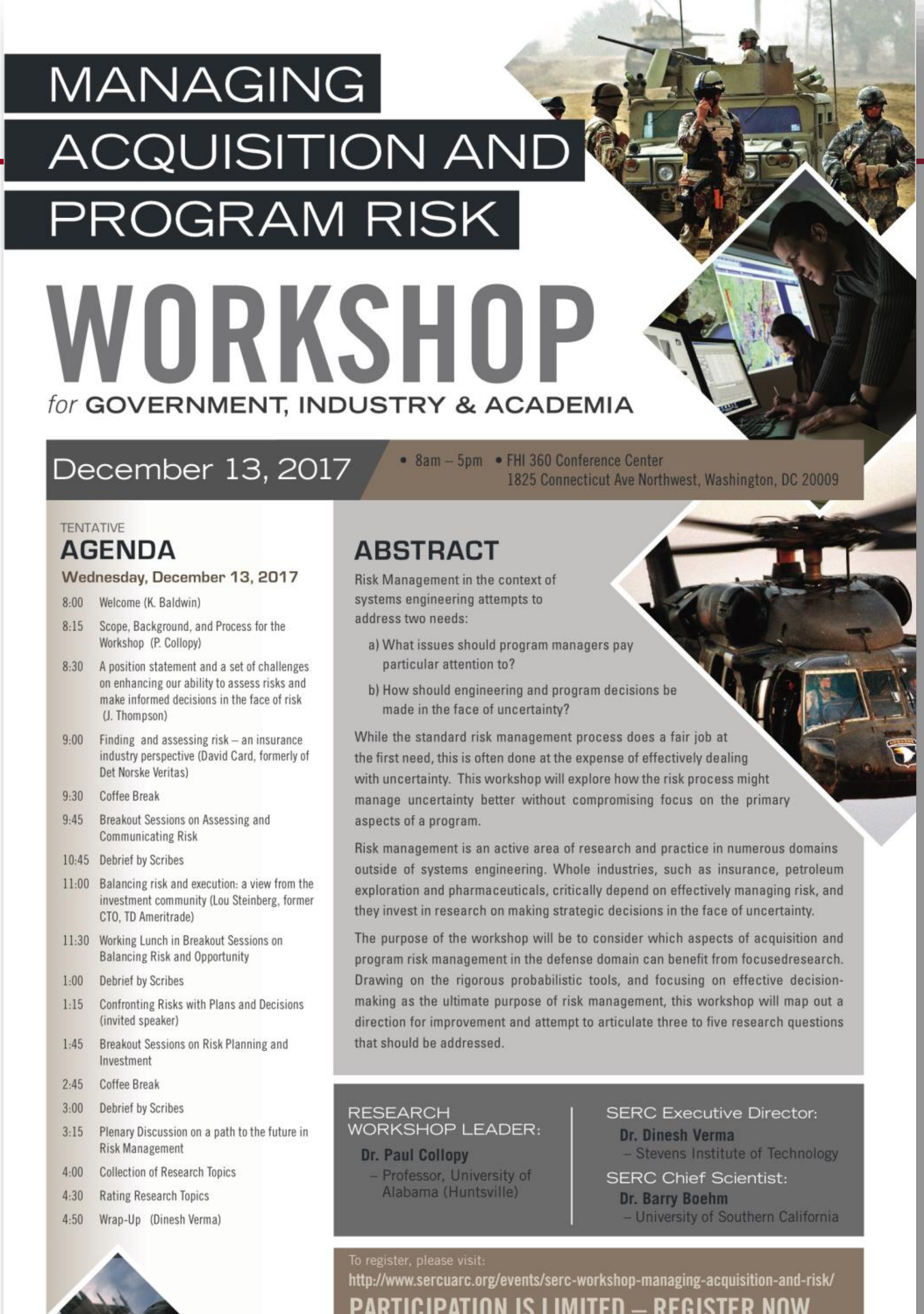
**DECEMBER 6-7, 2017**

**WORKSHOP ATTENDANCE IS BY INVITATION ONLY.**

**LOCATION:**

**20 F ST CONFERENCE CENTER**

**20 F STREET, NW**
**WASHINGTON, DC**



# MANAGING ACQUISITION AND PROGRAM RISK

# WORKSHOP

*for* GOVERNMENT, INDUSTRY & ACADEMIA

December 13, 2017

- 8am – 5pm
- FHI 360 Conference Center
  1825 Connecticut Ave Northwest, Washington, DC 20009

TENTATIVE

## AGENDA

**Wednesday, December 13, 2017**

8:00 Welcome (K. Baldwin)

8:15 Scope, Background, and Process for the Workshop (P. Collopy)

8:30 A position statement and a set of challenges on enhancing our ability to assess risks and make informed decisions in the face of risk (J. Thompson)

9:00 Finding and assessing risk – an insurance industry perspective (David Card, formerly of Det Norske Veritas)

9:30 Coffee Break

9:45 Breakout Sessions on Assessing and Communicating Risk

10:45 Debrief by Scribes

11:00 Balancing risk and execution: a view from the investment community (Lou Steinberg, former CTO, TD Ameritrade)

11:30 Working Lunch in Breakout Sessions on Balancing Risk and Opportunity

1:00 Debrief by Scribes

1:15 Confronting Risks with Plans and Decisions (invited speaker)

1:45 Breakout Sessions on Risk Planning and Investment

2:45 Coffee Break

3:00 Debrief by Scribes

3:15 Plenary Discussion on a path to the future in Risk Management

4:00 Collection of Research Topics

4:30 Rating Research Topics

4:50 Wrap-Up (Dinesh Verma)

## ABSTRACT

Risk Management in the context of systems engineering attempts to address two needs:

a) What issues should program managers pay particular attention to?

b) How should engineering and program decisions be made in the face of uncertainty?

While the standard risk management process does a fair job at the first need, this is often done at the expense of effectively dealing with uncertainty. This workshop will explore how the risk process might manage uncertainty better without compromising focus on the primary aspects of a program.

Risk management is an active area of research and practice in numerous domains outside of systems engineering. Whole industries, such as insurance, petroleum exploration and pharmaceuticals, critically depend on effectively managing risk, and they invest in research on making strategic decisions in the face of uncertainty.

The purpose of the workshop will be to consider which aspects of acquisition and program risk management in the defense domain can benefit from focusedresearch. Drawing on the rigorous probabilistic tools, and focusing on effective decision-making as the ultimate purpose of risk management, this workshop will map out a direction for improvement and attempt to articulate three to five research questions that should be addressed.

RESEARCH WORKSHOP LEADER:

**Dr. Paul Collopy**
– Professor, University of Alabama (Huntsville)

SERC Executive Director:

**Dr. Dinesh Verma**
– Stevens Institute of Technology

SERC Chief Scientist:

**Dr. Barry Boehm**
– University of Southern California

To register, please visit:
http://www.sercuarc.org/events/serc-workshop-managing-acquisition-and-risk/

PARTICIPATION IS LIMITED – REGISTER NOW

# Research workshops that we held (are going to hold) this year…

Cyber Resilient Weapon Systems Engineering Workforce Needs (in collaboration with MITRE)

Colloquium on Digital Engineering

Sensemaking (Sponsored by ODNI)

Continuous Development and Deployment (November 27 and 28, 2018)

# This is the context of the Pathfinder Project

Visit a number of warfare centers, R&D centers, National Laboratories, and FFRDCs, with the objective of talking to senior technical leaders – with a view to identify systems engineering "pain points", research priorities, and any strategic workforce considerations

**Almost 20 visits were completed…**

# Primary Questions and Research Priorities

- Modeling System Security, Risk, Reliability, and Resilience
  - Particular reference to Distributed Systems (IoT; Cyber-Physical Systems; Mission Threads)
- Agility at the scale of the Enterprise
- Mission Engineering -
  - Collaboration and Competition – Computational Policy Framework
- Knowledge Management
  - Legacy and into the future with changing demographics
- Model Based Engineering – Digital Engineering
  - Various sub-themes
- Analytics and Enhanced Quantification to all aspects of Systems Engineering
- Systems Engineering Aspects of Autonomy, AI, and ML, especially V&V
- “other topics”

# Modeling System Security, Risk, Reliability, and Resilience

- We need better models for complex, sensor-intensive cyber-physical weapon systems;
- How do we assess the risk/reliability of a mission? In particular, when we have an array of heterogeneous systems – some manned and some unmanned systems;
- We need models to assess and estimate the reliability of heterogeneous network centric systems;
- How do we do a vulnerability analysis for the prioritization of risk in system of systems?
- How to assess and model system security?
- How do we model and assess system security at scale?
- How do we model system resilience?
- How do we model system trust?
- There is a need for a holistic approach to assess and model system security, offensive cyber warfare, cyber-defense, and information security;
- How do you measure the security and resilience of a weapon systems?

# Primary Questions and Research Priorities

- Modeling System Security, Risk, Reliability, and Resilience
  - Particular reference to Distributed Systems (IoT; Cyber-Physical Systems; Mission Threads)
- Agility at the scale of the Enterprise
- Mission Engineering -
  - Collaboration and Competition – Computational Policy Framework
- Knowledge Management
  - Legacy and into the future with changing demographics
- Model Based Engineering – Digital Engineering
  - Various sub-themes
- Analytics and Enhanced Quantification to all aspects of Systems Engineering
- Systems Engineering Aspects of Autonomy, AI, and ML, especially V&V
- “other topics”

# Agility at the Scale of the Enterprise

- How do we balance risk, safety, and security on the one hand, and getting capability to the field in an accelerated manner?
- How do we address our acquisition culture, tradition, processes, governance, and procedure?
- How do we move from a policy and compliance culture to an incentive and outcome oriented culture?
- Error and fault monitoring are not able to keep up with the “speed of operations” – how do we fix this?
- Within an environment of extremely mission critical systems, how do we get better at trying new and different approaches?
- Tension between safety and agility – a paradox.  How best to rationalize this?
- How do we bring multiple disciplines, multiple doctrines, and multiple organizational cultures together to get through complex system and solution development faster?
- How do we fix an environment that lacks trust – between acquisition and contractors; between different organizations on the government side?
- We should question the relevant and value of ALL CDRLs, and make this lean.
- Can we do a risk and reward assessment of ALL SE steps – to allow more rapid development?
- Should we allow a more steam-lined and direct interplay between operators and users on the one hand; and developers and doctrine writers on the other?
- How do we evolve to bring greater agility in system development at the level of the enterprise?
- Modularity and Rapid Development:
  - Impact of Modularity on test and integration speed; and the need for comprehensive re-certification; Impact of modularity  - multiple case studies are necessary to understand cost and benefits, and impact of agile development, integration and test, and innovation.

# Primary Questions and Research Priorities

- Modeling System Security, Risk, Reliability, and Resilience
  - Particular reference to Distributed Systems (IoT; Cyber-Physical Systems; Mission Threads)
- Agility at the scale of the Enterprise
- Mission Engineering -
  - Collaboration and Competition – Computational Policy Framework
- Knowledge Management
  - Legacy and into the future with changing demographics
- Model Based Engineering – Digital Engineering
  - Various sub-themes
- Analytics and Enhanced Quantification to all aspects of Systems Engineering
- Systems Engineering Aspects of Autonomy, AI, and ML, especially V&V
- “other topics”

# Mission Engineering

- Tension between "owners" of systems and programs; and the "owners" of mission threads – we need to figure out a way to put incentives to align these two perspectives;
- What is the true cost of system integration? For standalone systems; and for the integration of a system into an enterprise.
- Mission analysis and engineering for complex system of systems – modeling and risk assessment;
- A mission thread cuts across multiple "lego pieces" in diverse geographical instances. How do we manage this enterprise when resources are allocated to the "lego pieces" and not to the mission threads?
- How do you characterize the "boundary of a system" when dealing with a system of multiple cloud based services? Furthermore, how do we develop a reference baseline for a "system in the field" when there are often local level variants to the designed or implemented baselines? This drives the integration of new services in the context of mission engineering.
- Integrated decision making and portfolio management:
  - How do we prioritize funding across multiple systems and programs for maximum impact on orthogonal mission threads?
  - Need an integrated decision framework (Space War-fighting Concept) spanning languages, cultures, doctrine across multiple organizations in a landscape that involves a diverse customer set (cultural inertia).
- Fleet level interoperability remains a challenge – particularly when dealing with concurrent and overlapping networks with conflicting information – this can and has compromised missions.
- Sometimes our requirements seem to go in one direction – from mission to system to sub-system – leading to a significantly reduced design space at the sub-system level and ultimately an underperforming system, and hence an underperforming mission. We need a better way.

# Primary Questions and Research Priorities

- Modeling System Security, Risk, Reliability, and Resilience
  - Particular reference to Distributed Systems (IoT; Cyber-Physical Systems; Mission Threads)
- Agility at the scale of the Enterprise
- Mission Engineering -
  - Collaboration and Competition – Computational Policy Framework
- Knowledge Management
  - Legacy and into the future with changing demographics
- Model Based Engineering – Digital Engineering
  - Various sub-themes
- Analytics and Enhanced Quantification to all aspects of Systems Engineering
- Systems Engineering Aspects of Autonomy, AI, and ML, especially V&V
- “other topics”

# Knowledge Management

- How do we capture our "design journey" on legacy systems and today's systems; our architecture; and our domain knowledge and heuristics in an actionable way for the future;  This is a real issue.
- One significant challenge is that we are using our systems way beyond their design life – how do we certify that what we have there is still good and will operate as intended?  This sometimes requires us to revisit a set of design and configuration decisions made 10-30 years ago.  How well do we know why the designs are the way they are?  While a number of our employees from 10-30 years ago are still with us – they are quickly retiring – and furthermore, today's generation is not that stable in the workplace.
- It is very easy to collect design and architecture information – but it is very hard to find it when you need it.  Our workforce is becoming very mobile, so there is a real need for us to figure this out soon.
- We need to develop a modern knowledge management and transfer system – we are truly in danger of loosing significant domain knowledge.

# Primary Questions and Research Priorities

- Modeling System Security, Risk, Reliability, and Resilience
  - Particular reference to Distributed Systems (IoT; Cyber-Physical Systems; Mission Threads)
- Agility at the scale of the Enterprise
- Mission Engineering -
  - Collaboration and Competition – Computational Policy Framework
- Knowledge Management
  - Legacy and into the future with changing demographics
- Model Based Engineering – Digital Engineering
  - Various sub-themes
- Analytics and Enhanced Quantification to all aspects of Systems Engineering
- Systems Engineering Aspects of Autonomy, AI, and ML, especially V&V
- “other topics”

# Model-Based Engineering: Digital Engineering

- We need help with translating natural language processing and design documents into MBE;
- Wish there was a practical notion of a roadmap; Further, how do we decide when should one begin modeling, when have we done enough modeling, and how much fidelity do we need and at what level and when?
- I wish we better understood the vast landscape of possible activities and scenarios and investments – and to identify the vector of maximum ROI when investing in MBE. We do not have the resources to do everything.
- I wish there was a decision framework for deciding where to go high fidelity and where to go low fidelity – otherwise we are just boiling the ocean.
- Has someone done an assessment of the skills and capabilities that we need to develop in support of digital engineering? This would be helpful.
- Model Based Testing:
  - How do we establish test boundaries for cyber-physical systems? Testing is too late for some system aspects. We need to get better at Simulation based Testing in support of mission engineering and interoperability; We need to better understand robustness and V&V associated with additive manufacturing. How do we do V&V and testing for learning systems?
- Validation, verification and accreditation of models:
  - What is sufficient? This is a rather labor intensive process. A key issue is model validation with sparse data. What tests are worth doing?
  - One challenge is model verification in the presence of small data sets;
  - Uncertainty quantification in multi-level modeling is a challenge for us.

# Primary Questions and Research Priorities

- Modeling System Security, Risk, Reliability, and Resilience
  - Particular reference to Distributed Systems (IoT; Cyber-Physical Systems; Mission Threads)
- Agility at the scale of the Enterprise
- Mission Engineering -
  - Collaboration and Competition – Computational Policy Framework
- Knowledge Management
  - Legacy and into the future with changing demographics
- Model Based Engineering – Digital Engineering
  - Various sub-themes
- Analytics and Enhanced Quantification to all aspects of Systems Engineering
- Systems Engineering Aspects of Autonomy, AI, and ML, especially V&V
- "other topics"

# Analytics and Enhanced Quantification to all aspects of Systems Engineering

- We need to cope with vast amounts of field data – such as condition based maintenance data from the fleet – our challenges are data science application to the army domain - data structuring, visualization, and analytics;
- How to we bring instrumentation and enhanced quantification to all aspects of systems engineering?
- Stockpile systems have collected tons of data – it would be nice to have applications of machine learning to find trends and patterns that the SMEs have not noticed and to even combine data from different weapon systems that share similar components and finding insights through machine learning;
- How do we compose and make consistent data from diverse sources?
- Can we instrument our infrastructure systems and development systems to provide real time data monitoring to increased insight into efficiency and effectiveness gains?
- Can we use system analytics and system instrumentation to develop the concept of a unique system DNA (wing number level)?
- Can we used machine learning applications focused on colleting and creating test metrics?

# Primary Questions and Research Priorities

- **Modeling System Security, Risk, Reliability, and Resilience**
  - **Particular reference to Distributed Systems (IoT; Cyber-Physical Systems; Mission Threads)**
- **Agility at the scale of the Enterprise**
- **Mission Engineering -**
  - **Collaboration and Competition – Computational Policy Framework**
- **Knowledge Management**
  - **Legacy and into the future with changing demographics**
- **Model Based Engineering – Digital Engineering**
  - **Various sub-themes**
- **Analytics and Enhanced Quantification to all aspects of Systems Engineering**
- **Systems Engineering Aspects of Autonomy, AI, and ML, especially V&V**
- **“other topics”**

# Systems Engineering aspects of AI, ML, and Autonomy

- We need to think about leveraging ML to collect and create metrics in support of Integration and Test;
- We need to develop applications such as Autonomous Topological Predictor-Corrector (UAS Testing);
- How do we setup boundary conditions between humans and machines? Pattern recognition is just scratching the surface; We need to focus more on algorithm development for decision processes – making decisions or advising decision makers; When we are wallowing in data, it would be good for AI/ML based systems to help us filter the wheat from the chaff. We need a research horizon that exceeds 3 to 4 years.
- AI in support of systems engineering and design: Explore the concept of developing cognitive agents to support designers and engineers. In particular, applying these agents to the notion of verification and validation.
- How do we do V&V for learning systems and self governing systems?
- Can ML help us bring quantification and analytics to all aspects of systems engineering?

# Primary Questions and Research Priorities

- **Modeling System Security, Risk, Reliability, and Resilience**
  - **Particular reference to Distributed Systems (IoT; Cyber-Physical Systems; Mission Threads)**
- **Agility at the scale of the Enterprise**
- **Mission Engineering -**
  - **Collaboration and Competition – Computational Policy Framework**
- **Knowledge Management**
  - **Legacy and into the future with changing demographics**
- **Model Based Engineering – Digital Engineering**
  - **Various sub-themes**
- **Analytics and Enhanced Quantification to all aspects of Systems Engineering**
- **Systems Engineering Aspects of Autonomy, AI, and ML, especially V&V**
- **“other topics”**

# “other topics”

- Set Based Design has a lot of potential – we just need better tooling to allow its robust implementation at scale;
- Requirements are written at the system and sub-system level, not at the mission level; optimization in done at the system and sub-system level, not at the mission level. This is a problem;
- We have to contend with Security Stovepipes – versus Security at the Mission Level (rather than a discrete system level) – particularly in Space;
- A pragmatic framework for the assessment, management, and leveraging of complexity – our complexity comes not just from the technical systems and associated dynamics, but also the dynamic regulatory environment. At an institutional level, another source of complexity is the diversity of our development and process frameworks, driven by the diversity of our customers.
- Requirements are getting out of hand – we are dealing with tens of thousands of requirements and it is only getting worse. Wish there was a better way.
- We need to better understand the SE related to integrating focused applications into a legacy enterprise; or integrating already built components – there is a need to build rigorous processes for integrating existing components into systems.

# Questions?