SYSTEMS ENGINEERING
Research Center

System 2020

Technical Report SERC-2012-TR-009-2

March 22, 2012

Principal Investigator: Dr. Stan Rifkin, Stevens Institute of Technology

Co-Principal Investigator: Dr. Barry Boehm, University of Southern California

Team Members:

Georgia Institute of Technology: Dr. William Rouse

Purdue University: Dr. Abhijit Deshmukh

Stevens Institute of Technology: Dr. Jon Wade

University of Alabama in Huntsville: Dr. Michael Griffin

University of Virginia: Dr. Barry Horowitz

Contract Number: H98230-08-D-0171 Task Order: 0002, DO 002, RT 020

Report No. SERC-2012-TR-009-2

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

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) under Contract H98230-08-D-0171 (Task Order 0002, DO 002, RT 020).

Any views, opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense nor ASD(R&E).

ABSTRACT

Systems 2020 is the research effort to answer a major portion of the challenge embodied in the DoD's science and technology priority for Engineered Resilient Systems (ERS). As a follow-on to the SERC's work in defining technical approaches for Systems 2020, DASD(SE) requested the SERC to work on two tasks. Task 1 involved working with Government research and engineering centers, and laboratories to characterize the design and systems engineering (SE) tools available to DoD projects, along with their potential for using these tools in integrated demonstrations of their capability to support representative future DoD systems acquisitions with respect to purpose, affordability, and interoperability. Task 2 involved identifying several design challenge problems to characterize the integrated environment capabilities being identified in Task 1.

Task 1 included visits to several DoD centers and laboratories; participation in several working group meetings for Systems 2020 and its extension to the Engineering Resilient Systems (ERS) initiative; and review of previous SERC and other tool assessments. It concluded that the purpose, affordability, and interoperability, as well as scalability of the computer-aided design (CAD) and SE tools available to DoD were weak with respect to the complexities of future DoD missions and net-centric systems of systems.

Based on discussion of the Task 1 analysis results with the sponsors, the original Task 2 statement was reinterpreted to involve the SERC Research Council in defining one or more representative future design challenge problems, and in determining key research ideas and directions that would enable DoD to cope with the challenges. This report includes the resulting two Grand Challenge scenarios of particularly difficult threat complexes beyond the reach of current tool support capabilities, with indications of the type of next-generation tools that would enable successful DoD responses. It also presents four high-leverage research areas that would be key to realizing the rapid and effective results described in the scenarios, using the Heilmeier criteria for evaluating proposed research initiatives:

- Affordability, Agility, and Resilience
- Enterprise Systems Engineering and Model Integration
- Trusted Systems and Cyber Security
- Human-Determined Systems

These were presented and discussed with the sponsors in a full-day offsite at the end of the study.

This Page Intentionally Left Blank

TABLE OF CONTENTS

FIGURES AND TABLES

1 SUMMARY

Systems 2020 is the research effort to answer a major portion of the challenge embodied in the DoD's science and technology priority for Engineered Resilient Systems (ERS). As a follow-on to the SERC's work in defining technical approaches for Systems 2020, DASD(SE) requested the SERC to work on two tasks. Task 1 involved working with Government research and engineering centers, and laboratories to characterize the design and systems engineering (SE) tools available to DoD projects, along with their potential for using these tools in integrated demonstrations of their capability to support representative future DoD systems acquisitions with respect to purpose, affordability, and interoperability. Task 2 involved identifying several design challenge problems to characterize the integrated environment capabilities being identified in Task 1.

Task 1 included visits to several DoD centers and laboratories; participation in several working group meetings for Systems 2020 and its extension to the Engineering Resilient Systems (ERS) initiative; and review of previous SERC and other tool assessments. It concluded that the purpose, affordability, and interoperability, as well as scalability of the computer-aided design (CAD) and SE tools available to DoD were weak with respect to the complexities of future DoD missions and net-centric systems of systems.

Based on discussion of the Task 1 analysis results with the sponsors, the original Task 2 statement was reinterpreted to involve the SERC Research Council in defining one or more representative future design challenge problems, and in determining key research ideas and directions that would enable DoD to cope with the challenges. This report includes the resulting two Grand Challenge scenarios of particularly difficult threat complexes beyond the reach of current tool support capabilities, with indications of the type of next-generation tools that would enable successful DoD responses. It also presents four high-leverage research areas that would be key to realizing the rapid and effective results described in the scenarios, using the Heilmeier criteria for evaluating proposed research initiatives:

- Affordability, Agility, and Resilience
- Enterprise Systems Engineering and Model Integration
- Trusted Systems and Cyber Security
- Human-Determined Systems

These were presented and discussed with the sponsors in a full-day offsite at the end of the study.

2 INTRODUCTION

Systems 2020 is the research effort to answer a major portion of the challenge embodied in the DoD's science and technology priority for Engineered Resilient Systems. This broader priority will develop, in this decade, engineering concepts, science, and design tools that enable defense systems to be resilient to attack and changes in the operational environment, and to develop agile design and manufacturing processes to enable systems to be rapidly reconfigured or adapted to new missions and threats. Systems 2020 is the research initiative that will provide new capabilities and approaches for faster delivery of flexible and adaptive systems that are trusted, assured, reliable, and interoperable with other systems to meet user needs.

DASD(SE) requested the SERC to work on two tasks. Task 1 involved working with Government research and engineering centers, and laboratories to characterize the design and systems engineering (SE) tools available to DoD projects, along with their potential for using these tools in integrated demonstrations of their capability to support representative future DoD systems acquisitions. The Task 1 results will be reported in Section 2.1. Task 2 involved identifying several design challenge problems to characterize the integrated environment capabilities being identified in Task 1. The Task 2 approach will be described in Section 2.2, and the results provided in Section 3.

2.1 TASK 1 STATEMENT AND RESULTS

The Task 1 statement is as follows:

Work with Government research and engineering centers, and laboratories performing Systems 2020 research in order to begin defining a library of computer aided design and systems engineering tools. There are two elements of this task:
(a) Characterize the purpose, affordability, interoperability and provider of off- the-shelf tools for design and engineering within the integrated environment being defined for Systems 2020;
(b) Characterize the potential for using these tools in integrated demonstrations of tradespace exploration, model- and platform- based design/analysis/testing, use of design patterns, and intelligent workflow sequencing across design and testing.

2.1.1 Task 1 Activity and Results

Dr. Rifkin visited several DoD centers and laboratories, and participated in several working group meetings for Systems 2020 and its extension to the Engineering Resilient Systems (ERS) initiative. He then worked with Dr. Boehm to relate the tool assessments to other SERC tool assessments performed under RT-MPT (SE Methods, Processes, and Tools Assessment), RT-9 (RT-MPT Phase 2), and 10 (SE Transformation), and to the assessments of future DoD SE tool needs in SERC RT-20 (Systems 2020 Strategic Initiative) Final Report, which also identified scalability to support the SE of increasingly complex DoD systems of systems as a critical needed capability along with purpose, affordability, and interoperability.

The resulting analysis produced the following assessment of the CAD and SE tools available to DoD with respect to their purpose, affordability, interoperability, and scalability:

- Their purpose is generally limited to individual domains: ground vehicles; space systems, high-performance computing, etc.
- Their affordability is generally acceptable within the domain, but it is expensive to tailor them to different or multiple domains.
- Their interoperability is largely acceptable within the domain, but it is difficult to interoperate them with tools in different or multiple domains.
- Their scalability is weak with respect to the complexities of future DoD missions and net-centric systems of systems.

Discussion of the Task 1 analysis results with the sponsors resulted in a reinterpretation of the original Task 2 statement, as discussed next.

2.2 Task 2 Statement and Results

Identify several design challenge problems to demonstrate the utility of the integrated environment being defined in Task 1. These design challenges should be relevant to Service needs and fully demonstrate the end-to-end capability of the integrated environment. These design challenges should be supported primarily with Service funding, with Systems 2020 supporting development of system engineering capabilities.

2.1.2 Task 2 Approach

The initial statement of Task 2 was as follows:
Identify several design challenge problems to demonstrate the utility of the integrated environment being defined in Task 1. These design challenges should be relevant to Service needs and fully demonstrate the end-to-end capability of the integrated environment. These

design challenges should be supported primarily with Service funding, with Systems 2020 supporting development of system engineering capabilities.

After discussion of the Task 1 analysis results with the sponsors, the original Task 2 statement was reinterpreted to involve the SERC Research Council (Drs. Deshmukh, Griffin, Horowitz, Rouse, and Wade, with Dr. Boehm as chair) in defining one or more representative future design challenge problems, and in determining key research ideas and directions that would enable DoD to cope with the challenges.

The results are shown in Section 3. Section 3.1 presents two Grand Challenge scenarios of particularly difficult threat complexes beyond the reach of current tool support capabilities, with indications of the type of next-generation tools that would enable successful DoD responses. The first scenario, A Different Type of Perfect Storm, initialized by Dr. Rouse and iterated by the Research Council members, emphasizes challenges of rapid and effective DoD interoperability with related agencies. The second scenario, Triple Threat and Triple Play, initialized by Dr. Boehm and iterated by the Research Council members, emphasizes challenges of rapid and effective internal-DoD interoperability.

Section 3.2 uses the Heilmeier criteria for evaluating proposed research initiatives to describe four high-leverage research areas that would be key to realizing the rapid and effective results described in the scenarios:

- Affordability, Agility, and Resilience
- Enterprise Systems Engineering and Model Integration
- Trusted Systems and Cyber Security
- Human-Determined Systems

These were presented and discussed with the sponsors in a full-day offsite at the end of the study.

3 GRAND CHALLNGE SCENARIOS AND HIGH-LEVERAGE RESEARCH AREAS

3.1 GRAND CHALLENGE SCENARIOS

3.1.1 A DIFFERENT TYPE OF PERFECT STORM

A DIFFERENT TYPE OF PERFECT STORM:

A VISION OF ACHIEVABLE FUTURE DoD SYSTEMS ENGINEERING CAPABILITIES

SERC Research Council
William Rouse, Lead Author

V 7.0, December 24, 2011

Situation

September 2025. Congress is back in session. The kids are back in school. The leaves are starting to change color. It seems like business as usual. It isn't.

There is a pending natural disaster in Washington, DC -- a category 5 hurricane is predicted to soon hit the mid-Atlantic coast. At the same time, advanced filtering and analysis of communications traffic and data from trillions of ultra small networked sensors have indicated the high likelihood of a terrorist attack focused on the food supply in Washington, DC and its surrounding suburban area. This attack appears to be part of a much broader offensive, in which the terrorist organization has acquired a nuclear device and a basic launch capability, and has it ready to launch from a remote location and explode it in a way that would take out Global Positioning Satellite (GPS) capability for a key period of time around the Washington DC hurricane and food supply attacks.

Capabilities

In contrast to the slow, inflexible, and uncoordinated responses to such crises and threats in the early 2000's, the rapid and effective response to the dual hurricane and terrorist threats is the result of significant research results in scalable, agile systems engineering (SE) methods applicable to both existing and new DoD platforms, SE collaboration methods, processes and tools (MPTs), and collaboration exercise capabilities and preparations. These initiatives were led by significant DoD investments in SE for rapid repurposing of existing DoD platforms and rapid crisis response capabilities, in collaboration with many other Federal, local government, and private organizations. These included FEMA, NOAA, DoD, the Red Cross, and other non-

governmental organizations (NGOs) to respond to the hurricane, and the Centers for Poison Control and Disease Control, FDA, FBI, DHS and DOD to respond to the suspected terrorist attacks.

As the inevitable result of public early warning communications, people across metro Washington, DC are queuing and rapidly emptying grocery store shelves while there are escalating updates on emergency room reports of symptoms of food poisoning. There is a deluge of moment-to-moment data, but the collaborative investments in data integration and need-to-know data sharing, along with the exercises in collaborative crisis response, have enabled the response organizations to rapidly converge on baseline strategic plans, and well-staffed and well-coordinated responsive action groups.

In response to the hurricane crisis, joint weather impact analysis systems originally developed for DoD operations have been collaboratively extended to determine the baseline needs for the various emergency evacuation, transportation, crime and fire damage containment, medical, communications, emergency housing and provisioning, and other response organizations, and baseline mobilization plans provided to reserve organizations such as the National Guard, Red Cross, and other governmental and non-governmental organizations for participation as needed. These organizations have participated in semi automated crisis-response exercises, which have not only improved the various organizations' collaboration effectiveness, but also have provided analyzable experience data for continuous crisis-response improvement, resulting in timely and highly effective minimization of the hurricane's damage. A key DoD contribution to damage minimization has been its improved SE capabilities for repurposing existing DoD ground, sea, and airborne platforms, enabling them to be rapidly reconfigured to provide improved flood control an emergency rescue capabilities.

Similar investments by DoD and its collaborators have created, exercised, and continuously improved similar capabilities for bringing together the key responders and improvised platforms and equipment for terrorist threats such as food poisoning and satellite attacks, and enabling them to develop and evolve baseline plans for countering the threats. These activities involve testing a range of leading indicators of possible evolutions of the terrorist attack, particularly those that involve the terrorists taking advantage of the rapidly approaching hurricane. This requires monitoring global communications of likely perpetrators including cellular calls, emails, texts and tweets, integrating this information with that from more traditional reconnaissance and surveillance platforms, and analyzing these multiple rapidly changing "stories" to infer adversaries' situation perceptions, changes of intentions, and emerging action plans that enable the response organizations to rapidly and effectively contain and defeat the terrorist activity. Key DoD contributions to neutralizing the food poisoning threat were its ability to rapidly reconfigure repurposed existing surveillance platforms and logistics platforms to monitor and diagnose the nature of the food poisoning threat, and to rapidly mobilize, deploy, and employ the medical capabilities necessary to minimize poison distribution and its effects.

For the DoD-intensive threat of disabling GPS capabilities via improvised launch of nuclear devices, DoD had developed, exercised, and evolved similar capabilities for neutralizing such threats. Using composable and adaptable fractionated satellite technology and a knowledge base on the vulnerabilities of the launch vehicle, a generation-after-next, rapid-virtual-collaboration, space-domain threat-response capability is able to rapidly design, program, and configure an in-orbit complex of detection, tracking, focusing, and power generation components to empower a set of spaceborne laser components to lock onto and cause the destruction of the launch vehicle when it is launched.

Critical Research and Investment

Achieving such capabilities by 2025 will require significant DoD investments, most critically in highly scalable and adaptable collaborative systems engineering capabilities. These need to be applied to cost-effectively repurpose existing DoD platforms to become more flexible and rapidly reconfigurable to meet unforeseen threats. To enable rapid and effective threat responses, SE capabilities need to bring together just the right participants to counter each threat, and to enable them to rapidly execute observe-orient-decide-act (OODA) loops to counter the initial threat, and to rapidly adapt to adversary counter-countermeasures. These capabilities will involve the systems engineering aspects of all of the DoD Science and Technology Emphasis Areas: Autonomy, Countering Weapons of Mass Destruction, Cyber Sciences, Data-to-Decisions, Electronic Warfare, Engineered Resilient Systems, and Human Systems.

The SERC Research Council has elaborated the contributions of key technologies needed for achieving the capabilities described above. These are discussed below under the categories of Enterprise and Model-Based SE, Agility and Affordability, Resilience and Flexibility, Cyber Security, Institutionalizing Elegant Design, Human Capital Development, and Human-Systems Integration.

Enterprise and Model-Based Systems Engineering

Achieving the above enterprise-level capabilities required several R&D accomplishments. The state of the art in model-based organizational simulation needed to be advanced in terms of interactive simulation environments with access to rich libraries of models for transformations, flows, uncertainty propagation, decision and action quality standards (e.g., rules of engagement), decisions and controls of phenomena ranging from the physical and informational to the behavioral and social. Data access and integration standards and algorithms were needed to parameterize models as well as support real-world deployment of model-based decisions. Methods for surmounting architectural incompatibilities across enterprises, in real-time, were needed to support access of information and communication of plans. Text analytics (e.g., data to decisions) needed to provide real-time automated inferencing of the organizational "stories" playing out. Knowledge of all of the above phenomena was quite extensive. Anticipation of scenarios like the above challenged our methods, tools, and computational environments to scale up for exploiting this knowledge.

Over a decade earlier, several agencies had started to invest in organizational simulation. The hand crafting of these types of simulations had made them expensive and time consuming to develop and deploy. Agencies invested in creating the now well-known OrgSim design architecture, libraries of component models, and development tools that enabled rapid and inexpensive prototyping of organizational simulations. The availability of this design infrastructure motivated a wide range of enterprises to develop simulations of their organizations. When coupled with technologies for immersive command posts or decision centers, OrgSim venues for enterprises became as common as flight simulators for the airlines and military. These venues now enable simulation-based strategic and tactical planning and execution.

Advanced sensing had been a priority for several decades. Ten plus years ago, this area morphed into pervasive sensing and analytics. The idea was to integrate "signals" from many more traditional sensors with new sources such as cell phones, email, texts, and twitter to form composite imagery of potential adversaries' activities, perceptions, and intentions. The goal was to rapidly transform this data into decisions on how to identify and counter adversaries, perhaps by attacking their intentions before they were translated into activities. Realizing this capability required tremendous advances in analytics, in part in signal processing but most of all in text analytics. Methods and tools were developed for meaning extraction from unstructured text in multiple languages across types of media. Commercial application of this technology to business intelligence by consumer products companies spawned the now famous "we know what you are thinking" spoof on Saturday Night Live.

All enterprises of any significant scope have long dealt with problems associated with IT integration across the disparate IT platforms of legacy systems, particularly during mergers and divestitures. Temporary mergers have always been most problematic because of the transitory nature of the integrated capability needed. This limits the time and money organizations are willing to invest. Various agencies invested in creating methods and tools for rapidly identifying

incompatibilities of data, processes, and architectures across different systems, as well as libraries of "plug-ins" that translate across these incompatibilities. These methods and tools included extensive knowledge management capabilities for exploiting lessons learned from past integration efforts. These developments enabled rapid and inexpensive temporary mergers of enterprises. These capabilities also revolutionized IT procurement by enabling smart buyers to understand in advance any difficulties in integrating new systems into existing IT infrastructures.

Within DoD, affordability considerations created the need to achieve new capabilities by repurposing existing physical platforms. New forms of model-based SE enabled the capture of models of these existing platforms (often confounded by differing patches or workarounds across the platform family), and the ability to perform rapid virtual-to-physical repurposing by exploring many virtual options, and progressing through increasingly-physical solutions. Enterprise-level virtual exercise and evaluation of the options also benefited from emerging capabilities in cross-model interoperability technology.

Agility and Affordability

As just discussed, achieving agility and affordability in repurposing physical platforms benefited much from rapid virtual-to-physical platform modeling and simulation capabilities. The speed of these capabilities was significantly enhanced by the use of multicore chips to evaluate numerous options in parallel.

The key to agility in complex crisis-response systems is for the participants to be able to operate via tacit interpersonal knowledge and interpersonal trust, as compared to basing collaboration on explicit documented knowledge among participants unfamiliar with working with one another. This implies not only developing powerful virtual collaboration capabilities, but also involving the participants in realistic collaboration exercises that build up tacit knowledge, mutual understanding, and trust.

In the 2025 scenarios above, this enabled participants from the various emergency response centers to log into a virtual collaboration room, to catch up on the status of the emergencies, and to discuss with the overall emergency-response leadership which of several detailed-response groups their organization should participate in. These would also tier down: the overall hurricane response team would have sub-teams for emergency evacuation, transportation, crime and fire damage containment, medical, communications, emergency housing and provisioning, and other response organizations, including those involved in rapidly repurposing physical platforms. Such scalable complexes of domain-specific collaboration needed significant research, exercise, and refinement to ensure their interoperability.

As a result, the participants are able to quickly determine which organization would take the lead on which response need, and to quickly negotiate response plans and resource contributions. And when unexpected new developments arose, they are able to quickly use their data gathering, analysis, visualization, and collaboration support tools to execute an OODA loop to coordinate a revised response.

In terms of affordability, there are clearly nontrivial investments in the development of scalable, interoperable, collaboration methods, processes, tools, data sources, models, exercise capabilities, and training capabilities. Further investments are needed for exercise development, operations, and analysis, and the creation and growth of a knowledge base of best practices and case studies for both continuous capability improvement and adaptation to new threats.

Major gains in affordability have been achieved by the gains in speed and effectiveness in repurposing existing DoD physical platforms, instead of expensive acquisition and maturing of new platforms. Additional significant gains have come from reductions in DoD labor costs via automation of previous human functions. Further, if one compares the efficiency and damage-avoidance in the 2025 scenario with the large expenditures and large damage losses of early-2000s crisis-response case studies, there would be a clearly high return on investment.

Such collaboration and analysis capabilities can also be applied to improve the affordability and total ownership costs of the acquisition of new systems as well, as shown in quantitative results from the SERC Valuing Flexibility study.

Resilience and Flexibility

The predictions generated by disaster response simulation models, and the *what-if* gaming exercises conducted by DoD and other agencies have been successful in identifying *a priori* several failure modes resulting from compound threats. Several critical failure modes arising from the confluence of a natural disaster and a coordinated terrorist attack have not been predicted. For example, the disruption in the incoming food supply due to the hurricane and the panic caused by it will completely alter the dynamics of the spread of the contaminated food. Preplanned approaches of isolating the source of contagion are not likely to be effective. The effective results of the Different Perfect Storm scenario above depend on a concerted effort in the defense and security agencies to develop systems and processes that are resilient to foreseen and unforeseen events. These systems have the capability to *be modified* or *modify themselves* quickly to meet a threat or make use of an opportunity that has not been anticipated.

Such resilience had been enabled by investments in architectures and component level capabilities, and by technological and human elements. All the technologies enabling resilience in systems, namely absorbing the change, being modified to meet the change, autonomously reconfiguring based on the change, adapting and evolving continuously based on learning, sending and predicting the environment, were evaluated and improved via modeling, simulation, and exercises, including those involved in repurposing existing DoD physical platforms to become more adaptable and resilient. For the hurricane and food poisoning scenarios, new protocols for traffic routing helped avoid cascading jams and clogging of the evacuation networks. Modular hand-held sensing devices provided a wide range of chemical, nuclear and biological detectors based on the latest available intelligence. Key commanders and decision-makers were trained to work with systems that are self-organizing and evolving as the situation unfolds.

The necessary R&D investments in understanding, measuring, valuing and incorporating adaptability, flexibility, reconfigurability, and self-organization into complex systems had paid off significantly. Not only were evacuation and rescue systems operated by variety of agencies able to inter-operate because of their modular architectures and standardized interfaces, but new sensing, surveillance, and satellite defense capabilities could be fielded in a matter of hours from constellations of composable satellite components. Self-organizing social networks, comprising of civilians and security personnel, provided reliable information flow channels to ensure effective command and control in this situation. New decision-making methods developed to manage resilience effectively were critical in ensuring that the response to the hurricane and the terrorist event would not degrade over time.

To cope with shrinking defense budgets, the procurement of these resilient systems was enabled by the ability of the DoD acquisitions community and government contractors to show positive returns on investment in reduced total ownership costs, to explicitly put a value on the additional dimensions of resilience and flexibility, and to conduct tradeoffs between resilience,

adaptability, flexibility, and other system performance measures such as cost, time, performance, usability and security.

Trusted Systems- Cyber Security

Another potential terrorist threat is a cyber attack in which our ships' turbines and other military vehicles suddenly stop working, weapon systems are disrupted, or our commanders' situational awareness displays start presenting misdirecting information. Cyber attackers will be capable of accomplishing such attacks, and even with the escalated attention paid to cyber security, our focus is on networks and not on the command and control or physical systems used in military operations.

Currently, cyber security is accomplished as a system perimeter protection function, consisting of the integration of selected available components for system user authentication, system access control, data encryption, etc. Recognized weaknesses of perimeter security solutions include:

- Access that attackers have to readily available security products, enabling their use as a support environment for exploit development
- The reuse of exploits by attackers for different systems using the same products for security
- Lack of protection for attacks that originate inside the protected system perimeter, such as insider or supply chain generated attacks.
- The lack of availability of application specific protection mechanisms for what system owners might consider the most critical subsystems requiring protection
- The separation between the information assurance, cyber security technical community and the application focused system engineering community.

Indications already exist that the future cyber attacks will include attacks on physical as well as IT systems. These physical systems include embedded software controllers and monitoring systems that can be manipulated by attackers. Attack targets can be expected to include the engines and turbines that propel military vehicles of all kinds, as well as weapon system control systems. As computer processing and networking continue to become more capable and economical, the desire to create agile and adaptive systems will continue to grow. Correspondingly, the software-controlled features in systems will increase and the opportunity for manipulating these features can be expected to grow as well. Cloud computing will permit a more centralized view of military conflicts and corresponding central control, on the one hand resulting in new cyber risks, and on the other hand providing opportunities for centralized resilience management solutions. These trends point to the need for protection beyond the perimeters of systems; protections that are embedded in the application itself and are designed based upon the detailed designs of the parts of systems being protected. Early research efforts point to the added security that can be afforded by what is referred to as system-aware security, including:

- Ability to combine techniques developed for the design of resilient systems with advanced cyber security techniques for achieving protection at the application layer of a system, including physical systems (e.g., use diverse redundancy for achieving

system continuity, and use configuration hopping with diverse redundant components for achieving moving target cyber security).
- Ability to utilize systems of systems design opportunities as a more resilient base for responding to cyber attacks.
- Ability to combine techniques developed for automatic control systems to determine if operator displays are being manipulated and also as a basis for making rapid forensic analyses after a cyber attack has possibly occurred (has a system been the victim of a cyber attack?).

Of course, a significant research effort would be required to develop a robust body of reusable design patterns for System Aware security solutions. While system-aware security offers a promising opportunity, it has its own set of weaknesses that need to be minimized:

- System-specific customized solutions would be required, although reusable design patterns could reduce the cost and time for developed solutions.
- The development process for application security software would need to be organized to utilize the tools for security applied by the cyber security software community, and the processes for user oriented response time employed by the application software community. One might argue that vulnerabilities in system-aware solutions would be a greater risk than vulnerabilities in perimeter solutions, and therefore software implementations would need even greater scrutiny.
- The system requirements process would need to be developed to include regularized methods for determining: a) what mixture of perimeter and application layer security is desired, b) what methods of evaluation of solutions should be utilized by system designers for presenting their solutions, c) what metrics should be utilized for both test and evaluation of such solutions. And, the evaluations tests and metrics would need to account for the integrated security provided by the mixture of perimeter solutions and system-aware solutions.

The needed systems engineering security research program would necessarily include efforts to:

- Expand the set of reusable design patterns for system aware security solutions and implement prototype capabilities with industry support.
- Develop evaluation methodologies and metrics that account for the integration of perimeter and system aware solution components
- Develop system of system, cloud-based resiliency solutions that take advantage of more centralized system configurations.
- Develop SW test and SW evaluation concepts that account for the risks of SW vulnerabilities as related to the security function being accomplished.

Institutionalizing Elegant Design

Systems of systems (SoSs) as complex as those supporting the Different Perfect Storm capabilities require SE teams that can collaborate in defining and designing SoSs with the conceptual integrity or design elegance to support several built-in sources of potential conflict.

These include supporting different mission needs, stakeholder value propositions, legacy systems, resource constraints, and emerging technologies, along with adapting to unforeseen circumstances such as adversary threats and changes in independently evolving component systems. Creating such SoSs requires levels of collaborative innovation beyond those currently practiced in DoD.

Some DoD initiatives such as the DoD Systems Engineering Guide for System of Systems begin to scope the problem by identifying such categories as Directed, Acknowledged, Collaborative, and Virtual SoSs, with the recognition that increasing departures from traditional SE practices are needed to cope with the challenges of increasing responsibility-authority mismatches. The 2025 Different Perfect Storm scenario assumes that considerable continuing progress has been made toward achieving such capabilities, although considerable further progress will need to be made to keep up with the challenges. Below is a summary of the issues involved.

If it is accepted that a core responsibility of the system engineer is the development of a product whose design may be said to possess the property of "elegance", and if we observe that this mandate is not widely accepted or even understood in the system engineering community today, then we must examine what might be required to institutionalize such a standard in the community. Broadly considered, the issue concerns both engineering culture and process. Both must be influenced if lasting change is to be effected.

Frosch in 1969 was apparently the first to offer the view that "design elegance" was the primary goal of system engineering as a discipline, and to place the responsibility for its attainment squarely at the feet of the system engineer. In a now-famous speech, he noted that

> "We have lost sight of the fact that engineering is an art, not a technique; technique is a tool. From time to time I am briefed on the results of a systems analysis or systems engineering job in a way that prompts me to ask the questions: 'That's fine, but is it a good system? Do you like it? Is it harmonious? Is it an elegant solution to a real problem?' For an answer I usually get a blank stare and a facial expression that suggests I have just said something really obscene."

However, Frosch did not attempt to parse the term "elegance", nor did he offer examples of systems that might be considered to possess, or not possess, that property. Writing two generations later, Griffin in 2010 endorsed Frosch's theme, noting that a half-century of system engineering process development and application has not obviously resulted in a reduction of large-scale system failures or cost and schedule overruns. He advocates a view of system engineering that is "beyond process", and in an extended discussion defines an elegant design as one possessing the attributes of effectiveness, robustness, efficiency, and minimization of unintended consequences (a.k.a. "good behavior").

While there has been support within the systems engineering community for these views, it remains true that generally agreed upon and quantifiable definitions of system effectiveness, robustness, etc., do not exist even with a given field (e.g., airplane, spacecraft, or submarine design), much less for broader classes of systems (e.g., missile defense, energy, transportation). Such definitions may generally exist at the engineering discipline level, such as for heat engines, wing sections, communications links, optimal filters, linear control systems, etc. However, complex engineered systems inherently incorporate the contributions of many such individual disciplines. There is as yet no accepted method of linking the various discipline criteria to describe, evaluate, and compare the properties of such systems as a whole. Analytical methods are an essential requirement for the development of a useful "theory of system engineering", a term employed here in a deliberate analogy to the broadly applicable theories which have evolved over the last two centuries in numerous engineering disciplines. The development of analytical criteria according to which different candidate system designs can be evaluated and compared will be essential if design elegance is to be institutionalized in practice.

When analytical measures applicable to engineering systems (as opposed to individual disciplines and sub-elements) do become available, even in their initially primitive form, it will be essential to incorporate their use in and application to new systems development. It will be required to incorporate these new methods into the formal system engineering process whose use will be required and championed by key customers, especially government customers.

Even today, most system engineers will be found to possess heuristic notions of system attributes such as "effectiveness", "robustness", and so on, and it will be generally agreed that such characteristics are to be encouraged. Yet one seeks in vain to find these criteria, however defined, used in the evaluation of system concepts or applied as "grading standards" in formal milestone reviews.

If these and other attributes are indeed thought to be measures of the elusive property we think of as "design elegance", and if we wish to "institutionalize" that property as a core measure of merit for system engineers and system engineering, then it is at the very least necessary so to inform the engineering community. This can only be done by customers, aided and abetted by those in the community who develop, maintain, promulgate, and evolve the base of engineering standards which, *in toto*, characterize engineering practice in any era.

A counterpart set of capabilities have used the research results on design elegance to address the problem of retrofitting design elegance into legacy platforms with brittle, point-solution, highly-patched architectures to enable the platforms to be rapidly repurposed to address Perfect Storm of other classes of crises or threats.

Human Capital Development

The conceptualization, development, deployment and maintenance of these systems required the existence of a capable and experienced technical workforce. Unfortunately, the demographic time bomb of the baby boomer generation technical workforce created a drought

of talent at specifically the same moment that demand for these skills was rapidly growing. These issues were recognized at the highest levels and the following actions were taken across the board to address these issues.

Systems thinking concepts are taught early in the academic training of our Nation's youth. This systemic approach was core in the instruction of science and technology, and is a fundamental component of project-based interdisciplinary instruction. Students complete a customized profile of their capabilities and early career objectives, if appropriate, that was used by an education/training management system to help tune their learning experiences throughout their career. Upon entering post-secondary training, students continued this multidisciplinary approach to systems while developing not only their technical skills, but also their ability to collaborate in cross-disciplinary teams, provide technical leadership, and develop the intuition and judgment to make system level trades. Many of the student's projects and assignments were based upon real world projects and challenges. The student's profile was updated accordingly and used to help pair them with work experiences outside of their academic institution. Academic and on the job training was blended such that they were reinforcing, both adding to the student's knowledge and experience base. Once entering the workforce, the profile was continued to be used for the learner's development. In addition to this, simulations were available which provided the "deliberate practice" that was necessary to build competence as well as the accelerated development of the necessary "scar tissue". These simulations were also used to educate and train new and existing teams of professionals as these factors can often be as critical as the capabilities of each individual on the team.

Breakthroughs in a number of critical areas of research were necessary to support these capabilities. Systems oriented curriculum needed to be developed and evaluated to provide systems thinking educational experiences at the earliest student ages. Research to determine what constituted deliberate practice for systems engineers and technical leaders with the results translated this into actionable curriculum, technology and training was critical. However, even with such a curriculum, there were major challenges in scaling the instruction. Some major impediments involved lack of resources, talented educational staff, and finally student demand. The future of STEM education was found to lie in the ability to conceive, develop, deploy and sustain experiential, interdisciplinary, massively customized instruction where the student is self-motivated and driven to learn, and is mentored by self-directed, motivated experts. The use of internet and networked technologies was critical to obviate limitations from geography and funding. In addition, "open-source" content and technology, coupled with social networking, was required to create a self-sustaining educational ecosystem of STEM and innovation excellence. A true education/training management system was required to provide an optimized, individualized learning experience.

Finally, there were the research challenges on how we could best provide a simulation environment such that individuals and teams can accelerate the learning of critical systems engineering competencies. This goal of providing realistic, emotionally engaging simulated experiences customized to the learner's specific needs was applied not only to a computer simulation, but also to live classroom simulations and experiences. Technology and tools were

also developed to efficiently capture the expertise of our rapidly retiring population of systems engineers and technical leaders so that these skills would not be lost to future generations. Research and development was effectively used to create an open environment so that the development efforts in this area can be leveraged to provide an evolving ecosystem of simulated experience development and support.

Human-Systems Integration

Many – though not all – of the response team members had years of practice using several modalities in situations where there were many simultaneous sources of possibly-conflicting data, many and geographically disparate stakeholders with various degrees of formality and hierarchy in their organizations, many different cultures and ways of interacting internally and externally, and many different ways of interacting in urgent, emergency and emerging situations.

The practices used computer-based simulations, red- vs. blue teams war games, small group exercises, large group exercises, and observing emergency teams in action (e.g., forest fire fighting, battlefield trauma treatment, aircraft carrier deck emergencies, SWAT teams, etc.). A set of protocols – a process handbook and organization structure – had emerged and been refined over the years. It was used by many field organizations, taught to many first responders, and tools and specialist methods were generally available to acquire, learn, and improve.

In particular, there were methods of:

- Quickly organizing teams from different heritages and incentive structures – such as law enforcement and military, paid vs. volunteer, active vs. reserve – by agreeing on a common set of rules.

- Helping leaders generate and trade off solutions by, among other things, evaluating whether and how much more intelligence and of which type to buy in this data-rich, information-poor environment, hampered by very limited channels due to the weather condition. These include quickly identifying suspect terrorist populations on which to focus the limited intelligence resources.

- Not reaching consensus too quickly (pressure to reach a quick consensus is a symptom of groupthink).

- Finding human resources from around the world to act as subject matter experts in accordance with the common operating rules. Such experts would include experts in rapidly repurposing physical assets to cost-effectively alleviate the crisis and counter the threats.

- Quickly surfacing reactions to solution scenarios, such as diverting traffic, conducting airport-style searches in certain places, detaining groups of people, using social media to communicate broadly, etc. These reactions are predicted based on detailed models of individual and group behavior that were developed in the 2010s as part of the then-seven DoD science and technology priority areas.

- Generating and evaluating trades in the political, economic, and community spaces, taking into consideration the multiplicity of objective functions seeking to be optimized. Economic trades included cost-effectiveness trades for rapidly reconfiguring hardware and software assets and evaluating their cost, schedule, and effectiveness impacts.

- Trading off group decision quality and speed, along with understanding the sources and impact of uncertainty in the emerging environment. One of the mechanisms the methods employed was varying the degrees of centralization and formalization, and looseness and tightness along the organizational control lines. These methods also clarified the operating rules for when there had to be meetings and collective agreement, and when decision authority could be pushed down to an individual level.

A big part of the creation of this relatively new corpus of managerial and organization knowledge was the combination of qualitative and quantitative, the attraction of sufficient numbers of people who stepped across the traditional boundaries of scholarly categories, and concrete recognition and reward for cross-disciplinary studies and research.

TRIPLE THREAT AND TRIPLE PLAY

A VISION OF ACHIEVABLE FUTURE DoD SYSTEMS ENGINEERING CAPABILITIES

SERC Research Council
Barry Boehm, Lead Author

V2 Draft 2, January 2, 2012

Situation

On September 4, 2026, intelligence sources learn of a major triple attack on DoD ground vehicles, air vehicles, and command centers in the Middle East. The attack is scheduled for 9/11/2026, the 25th anniversary of the Al Qaeda attack on New York and the Pentagon. The intelligence sources have learned that the anti-ground and anti-air missiles have a new, highly-accurate homing device and a warhead that is timed to go off just before impacting the target in a way that makes its kill probability near 100%. The command centers are vulnerable to a set of Trojan Horse codes that can be set off remotely to bring their data management systems down for at least an hour. The DoD has a week to neutralize all three components of this triple threat.

Capabilities

In contrast to some of the relatively slow and uncoordinated responses to single classes of threats in the early 2000's, the rapid and effective response to the triple threats of ground, air, and cyber attacks is the result of significant research results in scalable, agile systems engineering (SE) methods applicable to both existing and new DoD platforms, SE collaboration methods, processes and tools (MPTs), and collaboration exercise capabilities and preparations. These initiatives were led by significant DoD investments in SE for rapid repurposing of existing DoD platforms and rapid, SE-intensive crisis response capabilities.

There is a deluge of potentially-relevant data, but the collaborative investments in data integration and need-to-know data sharing, along with the exercises in collaborative crisis response, have enabled the response organizations to rapidly converge on baseline strategic plans, and well-staffed and well-coordinated responsive action groups.

By applying advanced human-directed associative and social-network based data analysis, the intelligence organizations have been able to identify and analyze test and performance data for the new threats. These have established that their lethal range is roughly 50 meters for ground vehicles and 100 meters for aircraft. They have determined the physics behind the

new homing devices, and have determined that a new virtual-presence device can identify and process the returns to the homing device sensor to convince the homing devices that the vehicles under attack are 100-150 meters behind where they actually are. By rapidly integrating and iterating a variety of models and running numerous options in parallel via multicore chips and cloud computing, they are able to go from simulating to testing the effectiveness of the virtual-presence devices, and to prepare various rapid-manufacturing facilities to produce enough ground and air versions of the virtual-presence devices to cover the area under threat.

A key DoD contribution to success had been its improved SE capabilities for repurposing existing DoD ground, sea, and airborne platforms, enabling them to be rapidly reconfigured to counter unforeseen threats. Thus, an initiative originally established to save money had turned into a major contributor to DoD rapid-response capability. A further key contribution had been the ability for diverse DoD organizations to participate in semi automated crisis-response exercises, which have not only improved the various organizations' collaboration effectiveness, but also have provided analyzable experience data for continuous crisis-response improvement, resulting in timely and highly effective crisis performance when needed.

In this situation, the virtual collaboration capabilities and associated model integration capabilities enabled the countermeasure designers, evaluators, testers, and users to rapidly evaluate, debug, and improve the virtual-presence devices, and to determine how best to plug them into the various vehicle ports and attach them to the vehicles for the best balance of endurance, effectiveness, and avoidance of adverse side effects. Additional collaborations involved the contributions of the candidate model-based rapid manufacturing organizations, the logistics organizations responsible for fielding and affixing the devices, and the training organizations for training users and operators in the use of the devices (including avoidance of follow-the-leader formations).

Within two days, the collaborations had determined and validated the viability of the concept and the models defining the manufacture, installation, and use of the ground and air devices on their platforms. This baseline enabled concurrent and incremental rapid manufacturing, transport, installation, and training in the devices' use. After six days, the ground and air vehicles in the area under threat were equipped with their devices, and the users were trained on the early-outfitted vehicles.

For the third-threat cyber attack, the knowledge that the command centers' data management systems (DMSs) were the target of the attack enabled the virtually-collaborating command center personnel and cyber security systems engineers to develop a system-aware point-solution defense for the DMSs.

After some suggested solutions, discussions, and modeling of options, the most attractive option was to replicate each DMS twice, and to place the original and two replicas between

two connectors in the command centers' software. The first connector would continue to invoke the original DMS in the same way, but would also invoke the replicas under different identities. Thus, if the original were disabled or subverted by the Trojan Horse software, the second connector would compare the results and use those of the replicas if something was different in the original. This solution was quickly developed, verified and validated, and electronically updated in the command centers' software.

As a result, on 9/11/2026, the anti-ground-vehicle and anti-air-vehicle missiles exploded harmlessly away from their targets, and the sources of the missile firings were tracked and successfully attacked. Similarly, the command centers' software execution was monitored and the Trojan Horse software was identified, eliminated, and analyzed for avoidance of future instances.

Critical Research and Investment

Achieving such capabilities by 2026 will require significant DoD investments, most critically in highly scalable and adaptable collaborative systems engineering capabilities. These need to be applied to cost-effectively repurpose existing DoD platforms to become more flexible and rapidly reconfigurable to meet unforeseen threats. To enable rapid and effective threat responses, SE capabilities need to bring together just the right participants to counter each threat, and to enable them to rapidly execute observe-orient-decide-act (OODA) loops to counter the initial threat, and to rapidly adapt to adversary counter-countermeasures. These capabilities will involve the systems engineering aspects of all of the DoD Science and Technology Emphasis Areas: Autonomy, Countering Weapons of Mass Destruction, Cyber Sciences, Data-to-Decisions, Electronic Warfare, Engineered Resilient Systems, and Human Systems.

The SERC Research Council has elaborated the contributions of key technologies needed for achieving the capabilities described above. These are discussed below under the categories of Enterprise and Systems of Systems SE and Model Integration; SE for Affordability, Agility, and Resilience; SE for Trusted Systems and Cyber Security; and SE for Human-Determined Systems.

Enterprise and Systems of Systems SE and Model Integration

Achieving the above enterprise-level capabilities required several R&D accomplishments. The state of the art in model-based organizational simulation needed to be advanced in terms of interactive simulation environments with access to rich libraries of models for transformations, flows, uncertainty propagation, decision and action quality standards (e.g., rules of engagement), decisions and controls of phenomena ranging from the physical and informational to the behavioral and social. Data access and integration standards, metadata, and algorithms were needed to parameterize and integrate models as well as support real-world deployment of model-based decisions.

Methods for surmounting architectural incompatibilities across enterprises, in real-time, were needed to support access of information and communication of plans. Text analytics (e.g., data to decisions) were needed to provide real-time automated identification of the test and performance data for the new threats. Knowledge of all of the above phenomena was quite extensive. Anticipation of scenarios like the above challenged our methods, tools, and computational environments to scale up for exploiting this knowledge. However, in many cases, the capabilities were able to "surf the technology waves" of increased multicore chip and cloud computing performance.

Over a decade earlier, several agencies had started to invest in organizational simulation. The hand crafting of these types of simulations had made them expensive and time consuming to develop and deploy. Agencies invested in creating the now well-known OrgSim design architecture, libraries of component models, and development tools that enabled rapid and inexpensive prototyping of organizational simulations. The availability of this design infrastructure motivated a wide range of enterprises to develop simulations of their organizations. When coupled with technologies for immersive command posts or decision centers, OrgSim venues for enterprises became as common as flight simulators for the airlines and military. These venues now enable simulation-based strategic and tactical planning and execution.

Advanced sensing had been a priority for several decades. Ten plus years ago, this area morphed into pervasive sensing and analytics. The idea was to integrate "signals" from many more traditional sensors with new sources such as cell phones, email, texts, and twitter to form composite imagery of potential adversaries' activities, perceptions, and intentions. The goal was to rapidly transform this data into decisions on how to identify and counter adversaries, perhaps by attacking their intentions before they were translated into activities. Realizing this capability required tremendous advances in analytics, in part in signal processing but most of all in text analytics. Methods and tools were developed for meaning extraction from unstructured text in multiple languages across types of media.

All enterprises of any significant scope have long dealt with problems associated with IT integration across the disparate IT platforms of legacy systems, particularly during mergers and divestitures. Temporary mergers have always been most problematic because of the transitory nature of the integrated capability needed. This limits the time and money organizations are willing to invest. Various agencies invested in creating methods and tools for rapidly identifying

incompatibilities of data, processes, and architectures across different systems, as well as libraries of "plug-ins" that translate across these incompatibilities. These methods and tools included extensive knowledge management capabilities for exploiting lessons learned from past integration efforts. These developments enabled rapid and inexpensive selective integration of DoD and external-organizations' IT assets. These capabilities also revolutionized IT procurement by enabling smart buyers to understand in advance any difficulties in integrating new systems into existing IT infrastructures.

Within DoD, affordability considerations created the need to achieve new capabilities by repurposing existing physical platforms. New forms of model-based SE enabled the capture of models of these existing platforms (often confounded by differing patches or workarounds across the platform family), and the ability to perform rapid virtual-to-physical repurposing by exploring many virtual options, and progressing through increasingly-physical solutions. Enterprise-level virtual exercise and evaluation of the options also benefited from emerging capabilities in cross-model interoperability technology.

Affordability, Agility, and Resilience

As just discussed, achieving agility and affordability in repurposing physical platforms benefited much from rapid virtual-to-physical platform modeling and simulation capabilities. The speed of these capabilities was significantly enhanced by the use of multicore chips to evaluate numerous options in parallel.

The key to agility in complex crisis-response systems is for the participants to be able to operate via tacit interpersonal knowledge and interpersonal trust, as compared to basing collaboration on explicit documented knowledge among participants unfamiliar with working with one another. This implies not only developing powerful virtual collaboration capabilities, but also involving the participants in realistic collaboration exercises that build up tacit knowledge, mutual understanding, and trust.

As a result, the participants are able to quickly determine which organization would take the lead on which response need, and to quickly negotiate response plans and resource contributions. And when unexpected new developments arose, they are able to quickly use their data gathering, analysis, visualization, and collaboration support tools to execute an OODA loop to coordinate a revised response.

In terms of affordability, there are clearly nontrivial investments in the development of scalable, interoperable, collaboration methods, processes, tools, data sources, models, exercise capabilities, and training capabilities. Further investments are needed for exercise development, operations, and analysis, and the creation and growth of a knowledge base of best practices and case studies for both continuous capability improvement and adaptation to new threats.

Major gains in affordability have been achieved by the gains in speed and effectiveness in repurposing existing DoD physical platforms, instead of expensive acquisition and maturing of new platforms. Additional significant gains have come from reductions in DoD labor costs via automation of previous human functions. Further, if one compares the efficiency and damage-avoidance in the multi-threat 2026 scenario with the large expenditures and large damage losses of early-2000s single-threat case studies, there would be a clearly high return on investment. Such collaboration and analysis capabilities can also be applied to improve the affordability and total ownership costs of the acquisition of new systems as well, as shown in

quantitative results from the SERC Valuing Flexibility study.

Increased system resilience had been enabled by investments in architectures and component level capabilities, and by technological and human elements. All the technologies enabling resilience in systems, namely absorbing the change, being modified to meet the change, autonomously reconfiguring based on the change, adapting and evolving continuously based on learning, sending and predicting the environment, were evaluated and improved via modeling, simulation, and exercises, including those involved in repurposing existing DoD physical platforms to become more adaptable and resilient.

The necessary R&D investments in understanding, measuring, valuing and incorporating resilience, performance, interoperability, usability, reliability, availability, maintainability, adaptability, flexibility, and reconfigurability into complex systems had paid off significantly. Not only were the various organizations' systems more resilient, cost-effective, and interoperable, but also they could be rapidly adapted to cope with both individual and multiple threats.

To cope with shrinking defense budgets, the procurement of these resilient systems was enabled by the ability of the DoD acquisition community and government contractors to show positive returns on investment in reduced total ownership costs, to explicitly put a value on the additional dimensions of resilience and flexibility, and to conduct tradeoffs between resilience, adaptability, flexibility, and other system performance measures such as cost, time, performance, usability and security.

Trusted Systems and Cyber Security.

Traditional cyber security was largely accomplished as a network-oriented or system perimeter protection function, consisting of the integration of selected available components for system user authentication, system access control, data encryption, etc. Recognized weaknesses of perimeter security solutions included:

- Access that attackers have to readily available security products, enabling their use as a support environment for exploit development
- The reuse of exploits by attackers for different systems using the same products for security
- Lack of protection for attacks that originate inside the protected system perimeter, such as insider or supply chain generated attacks.
- The lack of availability of application specific protection mechanisms for what system owners might consider the most critical subsystems requiring protection
- The separation between the information assurance, cyber security technical community and the application focused system engineering community.

Trends in system complexity and dynamism required further capabilities beyond network and perimeter defense. On the positive side, cloud computing permitted a more centralized view of military conflicts and corresponding central control, on the one hand resulting in new cyber risks, and on the other hand providing opportunities for centralized resilience management

solutions. These trends enabled approaches to protection beyond the perimeters of systems; protections that were embedded in the application itself and were designed based upon the detailed designs of the parts of systems being protected. For the 9/11/2026 scenario, the identification of the data management system as the most critical element needing protection suggested a point-defense approach associated with research in system-aware security, also including:

- Abilities to combine techniques developed for the design of resilient systems with advanced cyber security techniques for achieving protection at the application layer of a system, including physical systems (e.g., use diverse redundancy for achieving system continuity, and use configuration hopping with diverse redundant components for achieving moving target cyber security).
- Abilities to utilize systems of systems design opportunities as a more resilient base for responding to cyber attacks.
- Abilities to combine techniques developed for automatic control systems to determine if operator displays are being manipulated and also as a basis for making rapid forensic analyses after a cyber attack has possibly occurred (has a system been the victim of a cyber attack?).

The system-aware security research program included efforts to:

- Expand the set of reusable design patterns for system aware security solutions and implement prototype capabilities with industry support.
- Develop evaluation methodologies and metrics that account for the integration of perimeter and system aware solution components
- Develop system of system, cloud-based resiliency solutions that take advantage of more centralized system configurations.
- Develop SW test and SW evaluation concepts that account for the risks of SW vulnerabilities as related to the security function being accomplished.

Several additional SE-oriented trusted systems and cyber security research areas enabled stronger defenses against more complex threats. These included methods, processes, and tools for diagnosing and countering hardware security threats; for creating trusted systems from untrusted components; for using biological approaches for adaptive synthesis of attack antibodies; and for game-theoretic economic approaches for increasing attacker costs and risks.

Human-Determined Systems

Approaches to enterprise integration, affordability, resilience, and cyber defense involving autonomous agents, processing terabytes of data in microseconds and making system adaptation and execution decisions, provide tremendous opportunities for operating inside adversaries' OODA loops. However, there are several serious failure modes for autonomous systems (recognized in the DoD Science and Technology Emphasis Areas of Autonomy and Human Systems). These highlight the need for empowering humans to increase their ability to

achieve Human-Determined Systems by capitalizing on the strengths and avoiding the failure modes of the autonomous systems.
Examples of autonomy failure modes include system instability due to positive feedback; self modifying software that makes failures difficult to debug; weaknesses in commonsense reasoning about why human operators have made system control decisions; ability of multiple agents to make contradictory decisions about controlling the system; and vulnerability of autonomous agents to spoofing and misdirection.

In the 9/11/2026 example, human-determined system support included the advanced human-directed associative and social-network based data analysis used to identify and analyze test and performance data for the new threats. Particularly in the distribution and installation of the virtual-presence equipment, there were several critical challenges from the human perspective, primarily working cooperatively with many organizations that were different in every dimension. At the coarsest level, the United States had to work with Coalition and in-country partners. No two of them are alike and they are all different from the United States. At a slightly finer level, the military planners had to work with engineers, operators, contractors, administrators, and across all of the US Services and Agencies (Defense and Intelligence). And at the finest level of granularity, the work had to be conducted across individuals with different temperaments, paces of work (battle tempo), rewards, attention to detail, and trades of accuracy and immediacy, among many, many other factors.
One discovery during the Defense Industrial Base consolidation of the 1990s and 2000s that went unmined was the effect of combinations of different temperaments when, for example, an assembly line "metal-bender" would buy an innovative, creative organization in order to break into a growing market. The instance of remotely piloted vehicles (RPVs) became such a case study, where, for example, the one-paragraph DARPA "must have" list for Global Hawk would eventually run into problems with the full specification mentality of the manufacturing arm of the organization that bought the firm that won the Global Hawk development contract.
The turning point came later in the 2010s when it was observed that each of the temperaments one found in "nature" had a "home ground" (preferred place, "sweet spot") in the life cycle of major weapons systems. That is, innovation is critical at several points and attention to detail at several others. The research characterized the dimensions of the differences and then characterized the attributes most needed at each life cycle stage of development, manufacturing, operation, repair, provisioning, revision, etc. Organizations were then "slotted" into the places where they would make the greatest contribution and all organizations appreciated in detail the contributions of their upstream providers and downstream consumers.
This breakthrough countered a "one size fits all" trend. And it made possible thinking at the earliest possible stage about how to incorporate Middle Eastern field units, for example, into the physical deployment of countermeasures. The indigenous resources could be considered at the earliest moment for, say, distribution of the modified components in ground- and air-vehicles. How would Middle Eastern soldiers physically distribute all of the needed units and with a strong sense of urgency? How would one determine which ones could be trusted? Would there be a central pick-up place (hub and spoke) or saturation placement (everywhere

all at once, e.g., via air drop)? Would the units have to be encased in materials to absorb impact over in-country roads? Would weight be an issue? What if an enemy representative came into possession of a unit, a likely prospect? While this sounds like logistical thinking – and it is! – it is also distinctive of thinking about all of the disparate cultures at all levels one deals within any Area of Responsibility.

The research spanned the science and technology spectrum, investigating the considerable "sausage making" inherent in the years of examining what are essentially hidden group-level phenomena, concealed in unspoken narratives, hero stories, recognition ceremonies, working together conceptually and collaboratively, and other symbolic acts. Part of the groundwork for the coming together of examining group behavior to the benefit of DoD resilience was the late work of Minerva, a modest attempt to build a bridge between DoD and those interested in collective behavior.

The breakthrough was applied at all the levels: among engineers, among organizations, between Uniformed and Intelligence ranks, across Doctrine and Materiel, between US and foreign military organizations, and from Privates to Generals. One of the ways the research findings were made palatable and therefore easy to implement was that they were couched in the familiar terms of DOTMLPF because it was observed in the field that DOTMLPF nearly completely characterized the differences that needed to be aligned in order for the US DoD to be rapidly effective.

For example, nearly all Western militaries have special operations, wherein soldiers are given the broadest "Commander's intent" guidance and it is left to them to create the detailed plans and execute them. In other militaries, such autonomy, such loose connection between the commander and his/her troops is not a tradition. In other words, autonomy for special operations is doctrine, training, organization, personnel, and materiel in one type of military and the opposite in another.

The DOTMLPF perspective offered another, unexpected benefit: it helped to describe the boundary between man and machines. It had been an open and contentious question to decide where to draw the decision boundary between what humans were supposed to do and what machines were "responsible" for. Couching the boundary as movable, field-adaptable to each situation, based on the state of DOTMLPF, cleared the air for greater resilience and finding the best places in the life cycle for each possible combination along the boundary.
Getting the largest and the smallest groups to work together across all boundaries – on and off of the battlefield -- was seen as the ultimate force multiplier!
Within the DoD, the conceptualization, development, deployment and maintenance of these systems required the existence of a capable and experienced technical workforce. Unfortunately, the demographic time bomb of the baby boomer generation technical workforce created a drought of talent at specifically the same moment that demand for these skills was rapidly growing. These issues were recognized at the highest levels and the following actions were taken across the board to address these issues.

One key DoD imitative was the continuing and expansion of its efforts to introduce systems thinking concepts early in the academic training of our Nation's youth. This systemic approach was core in the instruction of science and technology, and is a fundamental component of project-based interdisciplinary instruction. Upon entering post-secondary training, students continued this multidisciplinary approach to systems while developing not only their technical skills, but also their ability to collaborate in cross-disciplinary teams, provide technical leadership, and develop the intuition and judgment to make system level trades. Many of the student's projects and assignments were based upon real world projects and challenges. The student's profile was updated accordingly and used to help pair them with work experiences outside of their academic institution.
In addition to this, simulations were available which provided the "deliberate practice" that was necessary to build competence as well as the accelerated development of the necessary "scar tissue". These simulations were originally developed for accelerating the SE competencies of individual DoD personnel, but were then extended in two key ways. One was to educate and train new and existing teams of diverse DoD personnel, as these factors can often be as critical as the capabilities of each individual on the team. The other was to generalize the capabilities to accelerate the individual and collaborative SE capabilities of the population at large.

Realizing these capabilities involved research challenges on how to best provide a simulation environment such that individuals and teams can accelerate the learning of critical systems engineering competencies. These challenges ranged from better understanding of the epistemology of holistic systems thinking, to the creation of improved virtual-reality learner-immersion technology. The resulting provision of realistic, emotionally engaging simulated experiences customized to the learner's specific needs was applied not only to a computer simulation, but also to live classroom simulations and experiences. Technology and tools were also developed to efficiently capture the expertise of our rapidly retiring population of systems engineers and technical leaders so that these skills would not be lost to future generations. Research and development was effectively used to create an open environment so that the development efforts in this area could be leveraged to provide an evolving ecosystem of simulated experience development and support.

Cross-Discipline Integration

The most critical success factor of all was the application of holistic systems thinking to the overall initiative of transforming DoD SE capabilities. This involved bringing the research and technology areas together in a continuing series of increasingly complex pilot projects and DoD-wide exercises to not only ensure that the area contributions were compatible and synergetic, but also to create a knowledge base of experience data on which technologies worked best in which situations, and on which aspects of the areas needed further research and integration to become more cost-effective.

This knowledge base was also used to support research and development of a useful "theory of system engineering", creating an analogy to the broadly applicable theories which have evolved over the last two centuries in numerous engineering disciplines. The development of analytical criteria according to which different candidate system designs can be evaluated and compared was essential to creating workable definitions of such terms as "design elegance."

When such analytical measures applicable to engineering systems (as opposed to individual disciplines and sub-elements) became available, even in their initially primitive form, their use was incorporated in and applied to new systems development. This generated a series of increasingly powerful and integrated SE methods, which were then incorporated into the formal DoD system engineering process, and subjected to continuing test, evaluation, and refinement to cope with the continuing DoD challenges of increasing system and environment scale, complexity, diversity, dynamism, and need for rapid and cost-effective mission performance.

3.2 Realizing the Scenario Results: High-Leverage Research Areas

Proposed SERC Grand Challenges: Responses to Heilmeier Questions

SERC Research Council, 2 January 2012

As a complement to the SERC Research Council DoD Systems Engineering (SE) Grand Challenges vision documents, " A Different Type of Perfect Storm" and "Triple Threat and Triple Play," this document provides responses to the Heilmeier questions for the four major initiatives in the vision document: SE for Affordability, Agility, and Resilience; Enterprise and Systems of Systems SE and Model Integration; SE for Trusted Systems and Cyber Security; and SE for Human-Determined Systems. We begin with SE for Affordability, Agility, and Resilience, as it provides context for the other three initiatives.

3.2.1 Affordability, Agility, and Resilience (Barry Boehm and Abhi Deshmukh, Leads)

Three of DoD's primary future challenges will be to field, operate, and support more affordable systems during a period of declining budgets; to evolve systems and personnel with the agility to respond to unforeseen threats within their adversaries' observe-orient-decide-act (OODA) loops; and the resilience of a family of products to serve effectively in a variety of alternative futures. Key to achieving these multiple conflicting challenges will be next-generation systems engineering (SE) capabilities that provide affordability, agility, and resilience not only to the fielded systems but also to the SE activity itself.

Below are answers to the Heilmeier questions for the proposed affordability, agility, and resilience initiative. It includes three primary sub-initiatives:

- SE for repurposing of existing DoD physical platforms and their associated software to avoid expensive new-system costs;
- SE for lean and agile definition, development, and evolution of affordable, agile, and resilient DoD multi-platform systems; and
- SE for tradeoff analysis and decision support for value-based balancing of affordability, agility, resilience, and other system performance and quality factors.

The initiative assumes that other SERC Grand Challenge initiatives are addressing:

- SE for enterprise and system-of-systems level challenges such as model integration, scalability, and cross-system change negotiation;
- SE for trusted systems and cyber security challenges such as system-aware security solutions; and
- SE for human-directed systems challenges such as human capital development, human-systems integration, and balancing of human direction and autonomous execution.

In return, this initiative will support the other initiatives by providing them with SE methods, processes, and tools for affordable, agile, and resilient achievement of their objectives, and for evaluating the tradeoffs among the resilience and other quality factors and the affordability and agility factors of their engineered systems.

1. What are you trying to do? Explain objectives using no jargon.

Each of the three sub-initiatives will be pursuing synchronized agendas over the first five years to develop, pilot, and refine initial capabilities that demonstrate significant improvements in affordability and agility for three pilot projects, as compared to traditional affordability and agility levels in the pilot domains. Their first two years will involve pilot-aware technology development. The third year will involve pilot-specific preparations for the three pilots while preserving domain-independent core capabilities, along with experiment design and instrumentation. The fourth year will involve execution, monitoring, and in-process refinement of the capabilities. The fifth year will involve pilot evaluations, pilot follow-ons, and preparation for more general long-range capabilities, including architecting of the common core capabilities to support multi-domain versions, and definition of research programs to address desired but immature capabilities.

The platform repurposing sub-initiative will extend and integrate current specialized platform-repurposing practices to concurrently address hardware, software, and human-factors considerations. It will also address the challenges of making the platforms support product lines, and of reverse engineering of legacy-platform hardware and software to determine the

most cost-effective ways to derive and implement a resilient platform architecture from a family of variously-patched, multi-version, brittle, point-solution platform instances.

The lean and agile system definition, development, and evolution sub-initiative will research and develop DoD-oriented decision aids for determining which forms of lean and agile development are best suited for which parts of a system, and will develop methods, processes, and tools for implementing and integrating the forms of development.

The value-based balancing of affordability, agility, resilience, and other system –ilities sub-initiative will research and develop DoD-oriented, value-based methods, processes, and tools for multi-criteria decision analysis (MCDA), including such key factors as total ownership cost and cost-of-delay.

2. How is it done today? What are the limits of current practice?

Many DoD legacy platforms minimized acquisition costs and have brittle, point-solution architectures. Over the years, they have undergone various specialized upgrades and ad-hoc patches, making the job of repurposing them or turning them into product-line platforms extremely difficult. Some excellent partial examples of platform repurposing exist, such as the TARDEC Versatile Ground Vehicles imitative supported by SERC and Wayne State University; the AMRDEC Prototype Integration Facility for aircraft and missile hardware; and the IBM VITA and SEI SMART service-oriented software re-engineering capabilities. But these have not been integrated into full-service hardware-software-human factors repurposing capabilities.

Pure agile methods rely on tacit interpersonal knowledge and have difficulties with scalability and high assurance. Architected agile methods have been shown to scale up to roughly 100-person software teams (e.g., the F-35 Autonomic Logistics Information System), but not beyond. Lean and Kanban methods work well for manufacturing, and are making progress in software development and post-deployment system evolution, but are not yet fully scalable or mature.

MCDA methods have been successfully applied in many relatively stable situations with small numbers of system parameters, operational scenarios, and mission stakeholders. But they face serious challenges as the numbers of parameters, scenarios, and stakeholders scale up and undergo rapid change, as with DoD systems of systems. Stakeholder value-based approaches provide ways to constrain or prioritize them and make decision analysis more tractable.

3. What's new in your approach? Why do you think it will be successful?

The SERC offers a new approach to university research with the following major advantages:

- The combined strengths of 20 leading, networked SE research universities;
- Strong connections to DoD via geography, previous collaborations, and DoD graduate schools;

- Strong track record of collaborative teaming on DoD research projects;
- Leading research in hardware and software platform re-engineering, via methods, processes, and tools for architectural style compatibility analysis and reconciliation, product line architectures, architecture recovery, and concurrent hardware, software, and human factors engineering, all of which need to be combined for successful platform repurposing;
- Leading research in application to varying DoD situations of lean and agile methods, including decision criteria for which parts of complex systems are best addressed by lean and agile methods, and formalization of hybrid solutions such as architected agile methods;
- Leading research in cost, schedule, and quality estimation for software, systems engineering, and systems of systems engineering, including tradeoffs among development cost, total ownership cost, development schedule, and system quality factors; and
- Early modeling of the use of multicore chips and cloud computing to rapidly evaluate numerous design and operational decision options to enable faster and more cost-effective systems engineering and operational decisions.

The SERC universities also have strong working connections with potential DoD piloting organizations, such as Wayne State with TACOM and TARDEC; UAH and Auburn with AMCOM/AMRDEC/MDA; Stevens with ARDEC; and USC with USAF/SMC; along with the built-in connections of the DoD Air Force Institute of Technology and the Naval Postgraduate School.

4. If you're successful, what difference will it make? To whom?

Currently, the DoD is challenged to react in a timely and effective fashion to an individual threat. The future is likely to involve multiple coordinated threats. The improved SE and operational agility resulting from the agility research will enable the DoD to more rapidly and effectively detect, understand, and neutralize future multiple coordinated threats, and generally to execute its observe-orient-decide-act (OODA) loops inside those of its adversaries. The affordability results will also enable the DoD to achieve these capabilities within smaller budgets, particularly by reducing total ownership costs and by rapidly repurposing existing platforms and systems to adapt to unforeseen threat circumstances. The resilience and –ility tradeoff results will enable DoD organizations to better balance their achievement of resilience and other priority needs. Particular organizations that have already shown interest in the SERC's capabilities in addressing DoD affordability, agility, and resilience include its two primary sponsors in sponsoring RT-18 on Valuing Flexibility, RT-24 on Model Integration, RT-25 on Net-Centric Requirements Determination, RT-30 on Rapid Conops Determination, and RT-35 on Agile and Lean SE. Other SERC sponsorship of affordability, agility, and resilience research has come from AFCAA's sponsorship of RT-6 on Next-Generation Software Cost Estimation, OSD/CAPE's co-sponsorship of RT-18 on Valuing Flexibility, TACOM's sponsorship of RT-26 on Vehicle Repurposing, the Army's sponsoring of RT-33 on Contingency Basing, and the Air Force SAF/AQR's sponsoring of RT-34 on Expedited SE.

5. What are the risks and the payoffs?

The major risks come from conflicting objectives. Simultaneously achieving scalability to numerous coordinating organizations and adaptation to rapid and often overlapping changes in threats, technology, missions, and the organizations themselves will strain the ability of systems of systems to cope with the complexity. Simultaneously achieving high agility via lightweight methods, and high assurance via more heavyweight methods, will present challenges, particularly when confounded with scalability and rapid overlapping changes. This highlights the need for deeper research in the interactions and tradeoffs among system and system-of-systems quality factors. Some aids in addressing these risks will be the ability to rapidly analyze more and more options via increasingly powerful multicore chips and cloud computing capabilities.

The main risk in platform repurposing is the cost and difficulty of creating a clean repurposed platform from a mongrel collection of diverse workarounds from an original hard-to-modify point solution platform. Extensions of SERC cost-of-modification estimation models will be developed to determine the conditions under which repurposing is cost-effective. Another source of risk is to entangle university professors and their come-and-go graduate students in the workload involved in the maintenance and support of the tools developed. Various strategies such as open-sourcing, copyrighting, copylefting, or licensing have been used by SERC universities to enable tool vendors to perform such support functions.

6. How much will it cost? How long will it take?

Below is a first-order budget for the first five years of the Affordability, Agility, and Resilience initiative, as outlined in the response to question 1. The Integration element covers both internal integration among the sub-elements and external integration with the other SERC Grand Challenge elements. The budget would reach a steady-state level of core funding of $5M/year by Year 4, which would involve a balanced mix of ongoing research and piloting of maturing capabilities. As with similar organizations such as the CMU Software Engineering Institute, the core-funded results would attract further funding and increased capabilities in the out-years.

Initiative Element / $K	Year 1	Year 2	Year 3	Year 4	Year 5
Platform Repurposing	1000	1500	2000	1000	1000
Lean and Agile Methods	600	900	1200	600	600
Value-Based Quality Factor Tradeoffs	600	900	1200	600	600
Integration	300	450	600	300	300
SERC Support of Pilots				2500	2500
Total	2500	3750	5000	5000	5000

Either at the beginning of Year 1 or as a run-up to the five-year activity, one or more workshops would be held to bring together researchers, sponsors, and prospective piloters and users of

the technology to review draft research plans, suggest improvements, and prioritize options based on degree of difficulty, near-term payoff, and long-term payoff. This would be followed by detailed planning, staffing, and organizing of the initiative elements. Each year would have mid-year and end-of-year workshops to review progress and make mid-course corrections.

7. What are the midterm and final "exams" to assess progress?

The first midterm would be a Piloting Readiness Review at the end of Year 2. Year 3 would involve working with the piloting organizations to tailor the technologies and prepare for the pilots, and Year 4 would involve running the pilots and again making mid-course corrections. Year 5 would involve pilot evaluations, pilot follow-ons, and preparation for more general long-range capabilities, including architecting of the common core capabilities to support multi-domain versions, and definition of research programs to address desired but immature capabilities. A second midterm would be held at the end of Year 5. It is envisioned that continuing midterms would be held in subsequent research and transition cycles.

3.2.2 Enterprise Systems Engineering and Model Integration (William Rouse, Lead)

Tangible Early Product(s): Product/Domain Model Interoperability Diagnosis and Integration Toolset

Realized 2026 Capability: Enterprise/SOS Full Model Integration, Change Propagation: Product, Process, Property, Domain, Mission, Environment

1. What are you trying to do? No jargon.

Enable rapid integration of computational models of complex public- private enterprises to support successful responses to the full range of 2026 scenarios, in particular cross-enterprise (SoS) collaborative negotiation, planning, and execution

2. How is it done today? What are the limits of current practice?

MS Excel, SysML, Process Edge, Model Center, AnyLogic, SPLASH

These are computational frameworks that enable programming and execution of multi-model representations, with capabilities ranging from basic (Excel) to sophisticated. They do not inherently resolve the central modeling issues articulated below. However, once these issues are addressed and resolved, these frameworks can be used to create computational instantiations of the resulting multi-level models.

3. What's new in your approach? Why do you think it will be successful?

Figure 1 illustrates our approach to multi-level modeling of complex public-private enterprises. This approach provides the basis for model integration and interoperability. Each level both enables and constrains the other levels. For example, if the ecosystem does not value and reward interoperability across elements of the enterprise, then the organizations in the system of systems will not invest in interoperability. Consequently, the interoperability of delivery operations will have received little attention. Work practices will, therefore, often be difficult and inefficient as the collective set of stakeholders at all levels have no incentives to pursue this goal.

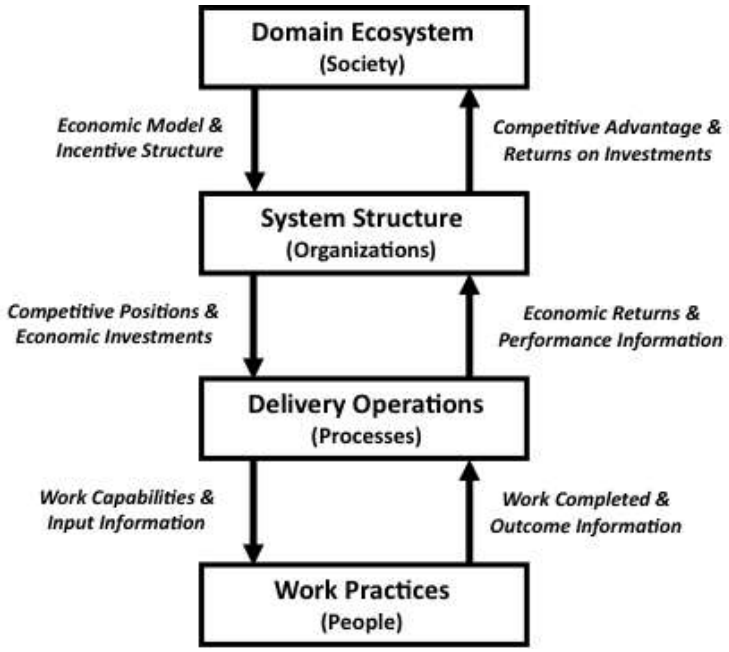

Figure 1. Multi-Level Modeling of Complex Public-Private Enterprises

Table 1 summarizes the fundamental modeling issues that must be addressed to achieve the goals of this initiative within the context of Figure 1.

Issue	Central Questions
Decomposition	What phenomena belong in each of the multiple levels? How does the representation of each phenomenon depend on its level?
Mapping	What variables cross levels between representations? What transformations are needed to connect across levels?
Scaling	What is the unit of scale for each phenomenon? By what quanta does each unit scale?
Approximation	What means are best used for data and computational efficiencies? What are the implications of choices, e.g., in terms of variance reduction?
Parameterization	How can data sets be accessed and normalized across elements of the enterprise? How can unbiased parameter estimates best be gleaned from the integrated data set?
Analytics	How changes of perceptions, intentions, and activities be inferred from large numeric and text data sets in real time? How can the time series of these "stories" be statistically evaluated for power and significance?
Curation	How can component models be represented, archived, maintained, and accesses to facilitate rapid model integration? How can participating organizations be incentivized to contribute to and make use of the curated archive?

Table 1. Fundamental Modeling Issues

This research will establish and validate a set of methods, processes, and tools for addressing the above issues, using the multi-level modeling framework to address contextually rich public-private enterprise scenarios for 2025. In early years these methods, processes, and tools will be prototypes; in later years, they will become more "industrial strength"

Success is predicated on our multi- university team having been involved in the evolution and maturation of this thinking for several decades, with application to defense, healthcare, and energy. This includes proven, successful applications at a significantly smaller scale than envisioned here, but at sufficient scale to serve as proofs of the concept.

4. If you are successful, what difference will it make? To whom?

Managers at all levels, ranging from operational field commanders to executive policy decision makers, will have well-informed inferences of stakeholders' perceptions, intentions, and activities, including inferred uncertainties, and principled deductions of the likely consequences of these perceptions, intentions, and activities across the large-scale public-private enterprise, including computationally propagated uncertainties. While "ground truth" is unknowable in complex socio-technical systems, these inferences and deductions will get one as close as possible to this holy grail. These capabilities will enable cross-enterprise (SoS) collaborative negotiation, planning, and execution.

5. What are the risks and the payoffs?

This initiative is very ambitious. However, much of what is being proposed is already being done, albeit often slowly and poorly, and always very expensively. There is little doubt that a principled approach can improve speed and quality at lower cost. Thus, the payoff across DoD can be immense and pervasive.

There are two overarching risks. First, the phenomena of interest are heavily laced with behavioral and social phenomena. Tremendous strides have been made in modeling such phenomena, but the level of maturity is not commensurate with modeling the physics of weapon systems. Second, adoption and use of the resulting principled approach must happen in the social, economic and political context of DoD. This "immune system" could reject this solution. Both risks are best addressable by thoughtful involvement of key stakeholder groups across academic disciplines and relevant organizations.

6. How much will it cost? How long will it take?

It will take 10 years and $20M to create a full, proven set of methods, processes, and tools for multi-level modeling of complex public- private enterprises. It will take an additional 3 years and $3M to train and educate a large cohort of users among DoD personnel and contractors. At that point, this transdisciplinary endeavor will have comparable maturity to semiconductor design today.

7. What are the midterm and final "exams" to assess progress?

Midterm No. 1: Compilation and elaboration of the state of knowledge and practice that will provide the building blocks of the proposed approach, including identification and refinement of best current capabilities. Validated via a series of workshops completed by the end of Year 2. This will also identify the lead candidates for stakeholder involvement for piloting the use of the best-available capabilities as part of the Year 3-5 Grand Challenge piloting activities.

Midterm No. 2: Development and demonstration of the proposed mechanisms for addressing the five modeling issues and two computational issues by the end of Year 5. A series of workshops will be used to engage stakeholders in applying these mechanisms to a set of well-defined complex public-private enterprise scenarios. This will also advance stakeholder involvement for piloting in the next rounds of piloting the Grand Challenge capabilities

Final Exam: Large-scale demonstration of the overall methods, processes, and tools to the National Level Exercise 2020. Lessons learned from this demonstration will be used to refine the packaging and usability of these methods, processes, and tools for completion in 2022, in time to begin the training and education elements of this initiative.

3.2.3 TRUSTED SYSTEMS AND CYBER SECURITY. (BARRY HOROWITZ, LEAD)

1. What are you trying to do? Explain objectives using no jargon.

The objectives of this initiative are to:

- Increase cyber security by developing new system engineering-based technology that provides a Point Defense option for cyber security
    - Inside the system being protected, for the most critical functions
    - Complements current defense approaches of network and perimeter cyber security
- Directly address supply chain and insider threats that perimeter security does not protect against
    - Including physical systems as well as information systems
- Provide technology design patterns that are reusable and address the assurance of data integrity and rapid forensics, as well as denial of service
- Develop a systems engineering scoring framework for evaluating cyber security architectures and what they protect, to arrive at the most cost-effective integrated solution.

2. How is it done today? What are the limits of current practice?

Current security protection is largely focused on network and perimeter defense, and reactive responses to exploited vulnerabilities, with relatively weak defense against attackers who have penetrated the perimeter.

3. What's new in your approach? Why do you think it will be successful?

The proposed initiative uses a system-aware security architecture approach to create stronger intra-perimeter defense of value-prioritized assets. It would combine design techniques from three communities: Cyber Security, Fault-Tolerant Systems, and Automatic Control Systems. The point defense solution designers would come from the communities related to system design, providing a new orientation to complement the established approaches of the information assurance community.

Some example techniques from each area are:

- Cyber Security: Data Provenance, Moving Target (Virtual Control for Hopping), and Forensics
- Fault-Tolerance: Diverse Redundancy (DoS, Automated Restoral), Redundant Component Voting (Data Integrity, Restoral)
- Automatic Control: Physical Control for Configuration Hopping (Moving Target, Restoral), State Estimation (Data Integrity), and System Identification (Tactical Forensics, Restoral).

This combination of solutions requires adversaries to expend significantly more resources to:

- Understand the details of how the targeted systems actually work
- Develop synchronized, distributed exploits
- Corrupt multiple supply chains

4. If you're successful, what difference will it make? To whom?

Cyber sciences are one of the seven DoD Science and Technology Emphasis Areas. Successful results would provide DoD-wide improvements in intra-perimeter cyber defense, strong disincentives for attackers due to higher attack expense levels, a system-aware architecture approach, and a knowledge base drawing on the scoring system that would expedite effective responses to new threats.

5. What are the risks and the payoffs?

Some unavoidable risks are the complications in dealing with security-porous legacy and commercial systems. Additional risks involve the need for balanced tradeoffs among security, performance, usability, interoperability, and other –ilities. Addressal of these risks will be factored into the architecting, analysis, scoring, test, and piloting of the research results.

The payoffs are summarized under question 4.

6. How much will it cost? How long will it take?

Roughly $2 million in year 1, rising to roughly $5 million/year in years 4 and 5 for piloting.

7. What are the midterm and final "exams" to assess progress?

Midterm exams would involve Piloting Technology Readiness Reviews at the end of year 2 and Piloting Readiness Reviews during years 3 and 4. Final exams would involve Piloting Results Reviews during years 4 and 5.

3.2.4 HUMAN-DETERMINED SYSTEMS (JON WADE AND STAN RIFKIN, LEADS)

In order to design, field, operate, and sustain better human-determined systems, the DoD needs extensive research and technology maturation in methods, processes, and tools for integrating human factors into systems engineering activities. This includes addressing the challenge of empowering humans to better monitor and guide the performance of autonomic systems to ensure avoidance of their potential failure modes. The 2007 National Research Council study report, Human-System Integration (HSI) in the System Development Process, provides an extensive agenda of candidate research activities oriented towards these needs. This proposed initiative extends the agenda to address further challenges of integrating human factors into DoD systems involving emerging technologies of social networking, autonomic smart systems, ultra large systems of systems, and virtual multi-discipline and multi-cultural collaboration capabilities.

Further, the DoD needs to support the development of human capital capable of reliably predicting the local and global impact of changes made to these systems from conception to obsolescence. This requires the ability to balance holistic and reductionist thinking, to view the system from many perspectives, and to have a depth of understanding of the non-linear cause and effects inherent in complex systems. These skills will be increasingly critical due to the need to repurpose existing DoD ground, sea, and airborne platforms, which provides greater systems challenges than the design from a blank sheet of paper. However, our current domestic educational system focuses primarily on breaking the system down and understanding the operation of the parts – reductionist thinking – and neglects to address the operation of the system as a whole including emergent properties of the system that do not exist in the parts alone – systems thinking.

We believe that DoD and the SERC can play important roles in advancing the future of grade-school to university science, technology, engineering and mathematics (STEM) education to enable the next generations of DoD-community personnel to integrate holistic systems thinking and systems engineering (SE) skills into their arsenal of knowledge, skills, and abilities. However, we recognize that the primary research and implementation of the STEM initiatives are external to ASD(R&E), and we have focused this part of the Human-Directed Systems initiative on relating its research results and capabilities to the overall objectives of the STEM initiative, while keeping the SERC universities in touch with further opportunities to execute SE portions of the STEM program.

We also believe that systems engineering and technical leadership involves workplace skills that go far beyond what can be taught effectively in academic institutions. We believe that by using technology we can create a simulation that will put the learner in an experiential, emotional state and effectively compress time and greatly accelerate the learning of a systems engineer faster than would occur naturally on the job.

Below are answers to the Heilmeier questions for the proposed initiative. Along with the continuing support of DoD SE participation in STEM initiatives, they include the following two sets of interdependent primary sub-initiatives:

1. HSI for Emerging Technologies
   1.1. Integrating human factors into DoD systems involving emerging new forms of cloud computing, social networking, autonomic smart systems, ultra large systems of systems, and virtual multi-discipline and multi-cultural collaboration capabilities;
   1.2. Empowering humans to better monitor and guide the performance of autonomic systems to ensure avoidance of their potential failure modes.
2. Experiential Learning Simulation
   2.1. Construction of what constitutes "deliberate practice" for systems engineers and systems thinkers and the resultant curriculum
   2.2. Development of simulation environment which can be used to accelerate the maturation of systems engineers and technical leadership.

This initiative will support the other initiatives by providing them with curriculum and training capabilities to create a workforce which is capable of supporting the newly developed SE methods, processes, and tools. .

1. What are you trying to do? Explain objectives using no jargon.

<u>HSI for Emerging Technologies</u>.

This research will integrate the results of case study analysis of experiences in performing HSI for emerging technologies, experimental prototyping of new approaches to HSI for emerging technologies, and pilot applications of the most promising approaches, to produce underlying principles, methods, processes, and tools that better empower humans to execute missions involving emerging technologies.

Experiential Learning Simulation

This research focus is on the development, deployment and evaluation of Experience Accelerator content and technology which is used to create an experiential, emotional state in the learner coupled with reflective learning so that time is effectively compressed and the learning process of a systems engineer and technical leaders is significantly accelerated as compared to the rate at which learning would occur naturally on the job. This work will build upon and expand research that is already being conducted in SERC RT16, and is targeted to result in a vibrant open source community which will expand the development and use of the technology throughout government, industry and academia. It will apply the accelerator capabilities to some of the participants in the Grand Challenge pilots to evaluate their effect on performance.

2. How is it done today? What are the limits of current practice?

Emerging technologies are often applied in the DoD during the period called by the Gartner Group the Peak of Inflated Expectations, involving adoption of immature technology and generally leading to disappointing results. Technology Readiness Levels of 5 or 6 for small applications are often assumed to apply to large, complex systems, which is generally not the case.

Post-academic training of systems engineers and technical leaders generally consists of the school of hard knocks in which the graduate is thrown into the foray of a major systems program and faced with the options of sink or swim. Unfortunately, the number of available programs in the DoD are diminishing, but their scale and criticality are increasing tremendously with the net result that there are fewer training grounds available to mature technical talent. The current process generally requires a technical staff to weather approximately three programs before they have risen up the maturity curve to the point where they can be considered senior technical leadership. Given the rate of technology change and the average time that people now spend in a career, this approach will not be successful moving forward.

3. What's new in your approach? Why do you think it will be successful?

Previous SERC university research efforts have investigated such emerging technologies as agile methods using combinations of case study analyses, multi-project experiments, and community workshops to determine the critical success factors and home grounds or sweet-spots for the technologies, and methods for determining appropriate combinations of the technologies that avoid overcommitment based on inflated expectations. The current SERC RT-35 on Lean and Agile SE is a representative extension of the approach to SE practices. Some early studies using the approach have been done for cloud computing and autonomic smart systems that would be extended, along with approaches for the other emerging technologies.

Our approach for the experience accelerator initiative leverages technology that has been successfully deployed in a number of different environments, including IT, social networking and serious gaming. In addition, the new approach is that of an open source movement in which the development costs can be distributed widely amongst a number of involved constituencies rather than using a limited proprietary approach which must be economically rewarding early in its development. These efforts will leverage the SERC network of more than 20 leading research universities to provide a basis for distributed development, piloting and evaluation of these technologies. It will also be leveraging existing research in these areas both within the SERC, but also across the great SERC collaboration community. Finally, with the maturation of the underlying technologies and the critical needs faced in education in these areas, the time is right for research and development supporting a new paradigm of education.

4. If you're successful, what difference will it make? To whom?

The triple threat scenario in the vision document includes extensive use of next-generation human collaboration capabilities that made a significant difference in the speed and effectiveness of the response to the threats. Overall, DoD and Services leaderships and their execution organizations are seriously concerned with the upcoming shortfall in DoD SE expertise.

Particular interest in the SERC's capabilities in addressing human resources include RT-1 BKCASE, RT-4 Technical Leadership Development, RT-16 Developing Systems Engineering Experience Accelerator (SEEA) Prototype and Roadmap, RT-19 Research on Building Education & Workforce Capacity in Systems Engineering, and RTs-35,36,37,and 39 on evaluating emerging technologies such as agile and lean methods, ultra large systems of systems, and cloud computing..

5. What are the risks and the payoffs?

The major risks come in the form of managing the scope of the program to what can be achieved in the desired timeframe, making the proper tradeoffs between long term technical architectures and short term prototypes, early exploratory studies and experiments vs. premature large-scale experiments. Many of these risks can be mitigated through the use of rapid prototyping and agile development techniques. The adoption challenges can be somewhat mitigated through the use of the broader SERC community to demonstrate and validate the capabilities, much as was done with RT-19.

The payoffs from enhanced education efficiency and effectiveness are transformational in nature, while not easily measured. The payoffs extend beyond the immediate threat to a more capable workforce; they occur at both the individual level of those who receive the education and training, but also at the national level in terms of our competitiveness on the world stage. Finally, the whole world will benefit in the improved educational capabilities.

6. How much will it cost? How long will it take?

Below is a first-order budget for the first five years of the Human Capital initiative, as outlined in the response to question 1. The Integration element covers both internal integration among the sub-elements and external integration with the other SERC Grand Challenge elements. The budget would reach a steady-state level of core funding of $5M/year by Year 4, which would involve a balanced mix of ongoing research and piloting of maturing capabilities. As with similar organizations such as the CMU Software Engineering Institute, the core-funded results would attract further funding and increased capabilities in the out-years.

Initiative Element / $K	Year 1	Year 2	Year 3	Year 4	Year 5
Human-Systems Integration	1000	1750	2500	1250	1250
Human-Systems Integration: Pilots				2000	2000
Experiential Learning Simulation	1000	1250	1500	750	750
Experiential Learning Simulation: Pilots		250	500	500	500
DoD SE Participation in STEM Initiatives	500	500	500	500	500
Total	2500	3750	5000	5000	5000

7. What are the midterm and final "exams" to assess progress?

For the HSI capabilities, Midterm 1 would be a Pilot Readiness Review to determine which capabilities would be ready and good matches to which classes of pilot projects. Midterm 2 would be an assessment of the results of the pilot applications. Subsequently, there would be a continuing series of readiness midterms and results midterms for increasingly ambitious pilot projects.

The Experience Accelerator sub-imitative is already on a path to perform pilots of initial capabilities as midterm exams, again followed by a continuing series of readiness midterms and results midterms for increasingly ambitious pilot projects.