ARJ

Defense Acquisition Research Journal

A Publication of the Defense Acquisition University

Achieving Dominant CAPABILITIES Through Technical EXCELLENCE *and* INNOVATION

2015

Hirsch Research Paper Competition

Presented on behalf of DAU by:

Defense Acquisition University

April 2015 Vol. 22 No. 2 | ISSUE 73

The Value of Training: Analysis of DAU's Requirements Management Training Results
Charles M. Court, Gregory B. Prothero, and Roy L. Wood

Increase Return on Investment of Software Development Life Cycle by Managing the Risk—A Case Study
William F. Kramer, Mehmet Sahinoglu, and David Ang

Manage Toward Success—Utilization of Analytics in Acquisition Decision Making
Sean Tzeng and K. C. Chang

Does Your Culture Encourage Innovation?
CDR Craig Whittinghill, USN, David Berkowitz, and Phillip A. Farrington

Online-only Article
DoD Comprehensive Military Unmanned Aerial Vehicle Smart Device Ground Control Station Threat Model
Katrina M. Mansfield, Timothy J. Eveleigh, Thomas H. Holzer, and Shahryar Sarkani

Article List

ARJ Extra

The Defense Acquisition Professional Reading List
Engineering the F-4 Phantom II: Parts into Systems
Written by Glenn E. Bugos
Reviewed by Lee Vinsel

Defense Acquisition Research Journal

A Publication of the Defense Acquisition University

Mr. Frank Kendall

Under Secretary of Defense for Acquisition, Technology, and Logistics

Mrs. Katharina G. McFarland

Assistant Secretary of Defense for Acquisition

Mr. James P. Woolsey

President, Defense Acquisition University

ISSN 2156-8391 (print) ISSN 2156-8405 (online)

The *Defense Acquisition Research Journal*, formerly the *Defense Acquisition Review Journal*, is published quarterly by the Defense Acquisition University (DAU) Press. Postage is paid at the U.S. Postal facility, Fort Belvoir, VA, and at additional U.S. Postal facilities. Postmaster, send address changes to: Editor, Defense Acquisition Research Journal, DAU Press, 9820 Belvoir Road, Suite 3, Fort Belvoir, VA 22060-5565. Some photos appearing in this publication may be digitally enhanced.

Articles represent the views of the authors and do not necessarily reflect the opinion of DAU or the Department of Defense.

Defense Acquisition University

Research Advisory Board

Mr. Patrick Fitzgerald
Defense Contract Audit Agency

Mr. Richard T. Ginman
Office of Defense Procurement and Acquisition Policy

Mr. Andre J. Gudger
Office of DoD Small Business Programs

Dr. Mary C. Redshaw
Dwight D. Eisenhower School for National Security and Resource Strategy

Ms. Heidi Shyu
Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology

Mr. James E. Thomsen
Office of the Assistant Secretary of the Navy for Research, Development and Acquisition

Dr. William A. LaPlante
Office of the Assistant Secretary of the Air Force for Acquisition

Editorial Board

Dr. Larrie D. Ferreiro
Chairman and Executive Editor

Mr. Richard Altieri
Dwight D. Eisenhower School for National Security and Resource Strategy

Dr. Michelle Bailey
Defense Acquisition University

Dr. Don Birchler
Center for Naval Analyses Corporation

Mr. Kevin Buck
The MITRE Corporation

Mr. John Cannaday
Defense Acquisition University

Dr. John M. Colombi
Air Force Institute of Technology

Dr. Neal Couture
The George Washington University

Dr. Richard Donnelly
The George Washington University

Dr. William T. Eliason
Dwight D. Eisenhower School for National Security and Resource Strategy

Dr. J. Ronald Fox
Harvard Business School

Dr. Jacques Gansler
University of Maryland

RADM James Greene, USN (Ret.)
Naval Postgraduate School

Dr. Ned Kock
Texas A&M International University

Dr. Mike Kotzian
Defense Acquisition University

Dr. Craig Lush
Defense Acquisition University

Dr. Andre Murphy
Defense Acquisition University

Dr. Christopher G. Pernin
RAND Corporation

Mr. Tim Shannon
Defense Acquisition University

Dr. Richard Shipe
Dwight D. Eisenhower School for National Security and Resource Strategy

Dr. Keith Snider
Naval Postgraduate School

Dr. John Snoderly
Defense Acquisition University

Ms. Dana Stewart
Defense Acquisition University

Dr. David M. Tate
Institute for Defense Analyses

Dr. Trevor Taylor
Cranfield University (UK)

Mr. Jerry Vandewiele
Defense Acquisition University

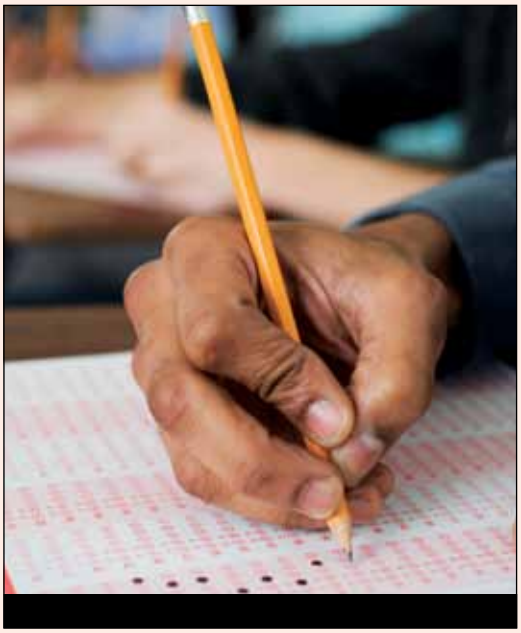
Dr. Roy L. Wood
Defense Acquisition University

Defense Acquisition Research Journal

A Publication of the Defense Acquisition University

Director, Visual Arts & Press	**Randy Weekes**
Managing Editor *Deputy Director,* *Visual Arts & Press*	**Norene L. Fagan-Blanch**
Assistant Editor	**Aleisha R. Jenkins-Bey**
Production Manager, *Visual Arts & Press*	**Frances Battle**
Art Director, *Visual Arts & Press*	**Harambee L. Dennis**
Lead Graphic Designer	**Diane Fleischer**
Graphic Designer	**Angie Brownie**
Technical Editor	**Collie J. Johnson**
Associate Editor	**Michael Shoemaker**
Copy Editor/Circulation Manager	**Debbie Gonzalez**
Multimedia Assistant	**Noelia Gamboa**
Editing, Design, and Layout	**The C3 Group** **Schatz Publishing Group**

CONTENTS | Featured Research



p. 154

The Value of Training: Analysis of DAU's Requirements Management Training Results

Charles M. Court, Gregory B. Prothero, and Roy L. Wood

This article examines assumptions and measures student progress at the Defense Acquisition University's Advanced Concepts and Skills for Requirements Management course, RQM 310, using pre- and post-testing data analyzed through SPSS t-tests or analysis of variation.

p. 174

Increase Return on Investment of Software Development Life Cycle by Managing the Risk—A Case Study

William F. Kramer, Mehmet Sahinoglu, and David Ang

This case study uses modeling and simulation to depict the cost of risk associated with the "Waterfall" approach for a proposed Software Development Life Cycle. The unforeseen risk is shown to produce a Return on Investment when the proper resources are aligned.

p. **192**

Manage Toward Success—Utilization of Analytics in Acquisition Decision Making

Sean Tzeng and K. C. Chang

Defense Business System Acquisition Probability of Success is an analytic model that represents a way ahead to support acquisition decision making, and an initial step forward in improving human understanding and ability to innovate and engineer systems though evidential reasoning.

p. **216**

Does Your Culture Encourage Innovation?

CDR Craig Whittinghill, USN, David Berkowitz, and Phillip A. Farrington

The authors examine culture within an organization and how it can be modified to improve innovativeness and overcome future/emerging threats to meet new and complex challenges.

CONTENTS | Featured Research

p. **240**

DoD Comprehensive Military Unmanned Aerial Vehicle Smart Device Ground Control Station Threat Model

Katrina M. Mansfield, Timothy J. Eveleigh, Thomas H. Holzer, and Shahryar Sarkani

The robust threat model the authors propose addresses cybersecurity threats to a complete Unmanned Aerial System (hardware, software, communication network) and the associated human threats. The full version of this article appears in the online edition of this issue of the *Defense ARJ*.

http://www.dau.mil/publications/DefenseARJ/default.aspx

p. viii

Call for Authors

We are currently soliciting articles and subject matter experts for the 2015–2016 *Defense Acquisition Research Journal* print years.

p. 274

Professional Reading List

Engineering the F-4 Phantom II: Parts into Systems
Written by Glenn E. Bugos, Reviewed by Lee Vinsel.

p. 276

Defense ARJ **Guidelines for Contributors**

The Defense Acquisition Research Journal is a scholarly peer-reviewed journal published by the Defense Acquisition University. All submissions receive a blind review to ensure impartial evaluation.

p. 284

Defense Acquisition University Web Site

Your online access to acquisition research, consulting, information, and course offerings.

p. 285

***Defense ARJ* Survey**

We want to know what you think about the content published in the *Defense Acquisition Research Journal.*

CALL FOR AUTHORS

We are currently soliciting articles and subject matter experts for the 2015–2016 *Defense Acquisition Research Journal* (*ARJ*) print years. Please see our guidelines for contributors for submission deadlines.

Even if your agency does not require you to publish, consider these career-enhancing possibilities:

- Share your acquisition research results with the Acquisition, Technology, and Logistics (AT&L) community.
- Change the way Department of Defense (DoD) does business.
- Help others avoid pitfalls with lessons learned or best practices from your project or program.
- Teach others with a step-by-step tutorial on a process or approach.
- Share new information that your program has uncovered or discovered through the implementation of new initiatives.
- Condense your graduate project into something beneficial to acquisition professionals.

ENJOY THESE BENEFITS:

- Earn 25 continuous learning points for publishing in a refereed journal.
- Get promoted or rewarded.
- Become part of a focus group sharing similar interests.
- Become a nationally recognized expert in your field or speciality.
- Be asked to speak at a conference or symposium.

We welcome submissions from anyone involved with or interested in the defense acquisition process—the conceptualization, initiation, design, testing, contracting, production, deployment, logistics support, modification, and disposal of weapons and other systems, supplies, or services (including construction) needed by the DoD, or intended for use to support military missions.

If you are interested, contact the Defense ARJ *managing editor (**DefenseARJ@dau.mil**) and provide contact information and a brief description of your article. Please visit the* Defense ARJ *Guidelines for Contributors at **http://www.dau.mil/pubscats/Pages/ARJ.aspx**.*

FROM THE CHAIRMAN AND EXECUTIVE EDITOR

Dr. Larrie D. Ferreiro

The theme for this edition of *Defense Acquisition Research Journal* is "Achieving Dominant Capabilities through Technical Excellence and Innovation," which is the theme for the 2015 DAU Training Symposium presented by the Defense Acquisition University Alumni Association (DAUAA). The DAUAA sponsors the annual Hirsch Research Paper competition, and the winners of the award for 2015 are: First Place "The Value of Training: Analysis of DAU's Requirements Management Training Results," by Charles M. Court, Gregory B. Prothero, and Roy L. Wood; and Second Place "Increase Return on Investment of Software Development Life Cycle by Managing the Risk—A Case Study," by William F. Kramer, Mehmet Sahinoglu, and David Ang. We congratulate both teams of winners, who were selected from a competitive field of entrants.

The "Value of Training" article, as the title indicates, posits that classroom training of the type conducted at the Defense Acquisition University noticeably increases a student's learning, and at the same time lays to rest several long-held assumptions about differences in the learning capability of different demographic groups—inside versus outside the Beltway, time in billet, etc. The "Increase Return on Investment" article examines the use of statistical methods to examine software error rates, allowing a better estimation of the return on investment during the software development life cycle.

Two other articles are included in the print and online editions of this issue: "Manage Toward Success—Utilization of Analytics in Acquisition Decision Making," by Sean Tzeng and K. C. Chang; and "Does Your Culture Encourage Innovation?" by CDR Craig Whittinghill, USN, David Berkowitz, and Phillip A. Farrington. The article "Manage Toward Success" proposes a statistical methodology called Bayesian analysis to orient the enormous amount of acquisition data and evidence to support decision making. "Does Your Culture Encourage Innovation?" reports the results of a University of Alabama study of the Department of Defense culture at the organizational level, and proposes changes to enable it to communicate and act rapidly, and to innovate.

The paper "DoD Comprehensive Military Unmanned Aerial Vehicle Smart Device Ground Control Station Threat Model" by Katrina M. Mansfield, Timothy J. Eveleigh, Thomas H. Holzer, and Shahryar Sarkani analyzes the cybersecurity vulnerabilities of handheld UAV ground control stations in order to enhance their security and operational environment. The full version appears in the online edition of this *Journal* (Issue 73).

The featured book in this issue's Defense Acquisition Professional Reading List is Glenn E. Bugos's *Engineering the F-4 Phantom II: Parts into Systems*, reviewed by Lee Vinsel.

Finally, the *Defense Acquisition Research Journal* masthead continues to evolve. For our Editorial Board, we note that Aude-Emmanuelle Fleurant has departed her position, and we acknowledge her contributions to the *Defense ARJ*. At the same time, we welcome to the Board Dr. William T. Eliason from the Dwight D. Eisenhower School for National Security and Resource Strategy. On our Research Advisory Board, we note that Dr. Nayantara Hensel and Mr. Brett B. Lambert have left their positions. We wish them well and thank them for their help.

On a personal note, I am pleased to welcome Dr. Mary Redshaw to the Research Advisory Board. Having left her position at the Defense Acquisition University, where among many other things she served as the Deputy Executive Editor of the *Defense ARJ* and my right hand, she has joined the faculty at the Dwight D. Eisenhower School. I am very glad to still be able to call on her wisdom and experience when needed.

DAU CENTER FOR DEFENSE ACQUISITION RESEARCH

RESEARCH AGENDA 2015

The Defense Acquisition Research Agenda is intended to make researchers aware of the topics that are, or should be, of particular concern to the broader defense acquisition community throughout the government, academic, and industrial sectors. The purpose of conducting research in these areas is to provide solid, empirically based findings to create a broad body of knowledge that can inform the development of policies, procedures, and processes in defense acquisition, and to help shape the thought leadership for the acquisition community.

Each issue of the *Defense ARJ* will include a different selection of research topics from the overall agenda, which is at: http://www.dau.mil/research/Pages/researchareas.aspx

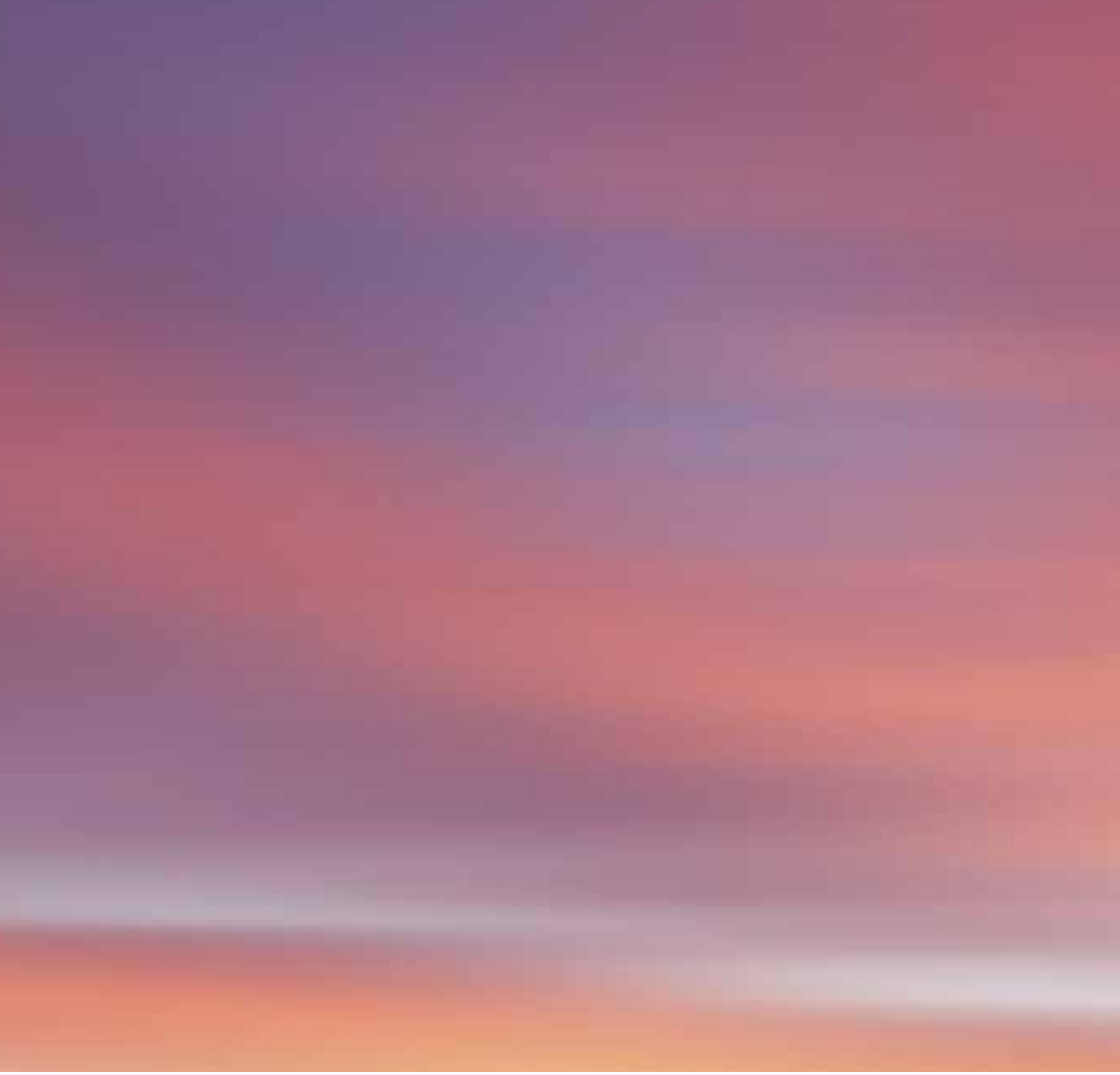
Measuring the Effects of Competition

- What means are there (or can be developed) to measure the effect on defense acquisition costs of maintaining an industrial base in various sectors?
- What means exist (or can be developed) of measuring the effect of utilizing defense industrial infrastructure for commercial manufacture in growth industries? In other words, can we measure the effect of using defense manufacturing to expand the buyer base?

- What means exist (or can be developed) to determine the degree of openness that exists in competitive awards?
- What are the different effects of the two best-value source-selection processes (tradeoff vs. lowest price technically acceptable) on program cost, schedule, and performance?

Strategic Competition

- Is there evidence that competition between system portfolios is an effective means of controlling price and costs?
- Does lack of competition automatically mean higher prices? For example, is there evidence that sole source can result in lower overall administrative costs at both the government and industry levels, to the effect of lowering total costs?
- What are the long-term historical trends for competition guidance and practice in defense acquisition policies and practices?
- To what extent are contracts being awarded noncompetitively by congressional mandate, for policy interest reasons? What is the effect on contract price and performance?
- What means are there (or can be developed) to determine the degree to which competitive program costs are negatively affected by laws and regulations such as the Berry Amendment and Buy American Act?



ISSUE 73
APRIL 2015
VOL. 22 NO. 2

We're on the Web at:
http://www.dau.mil/pubscats/Pages/ARJ.aspx

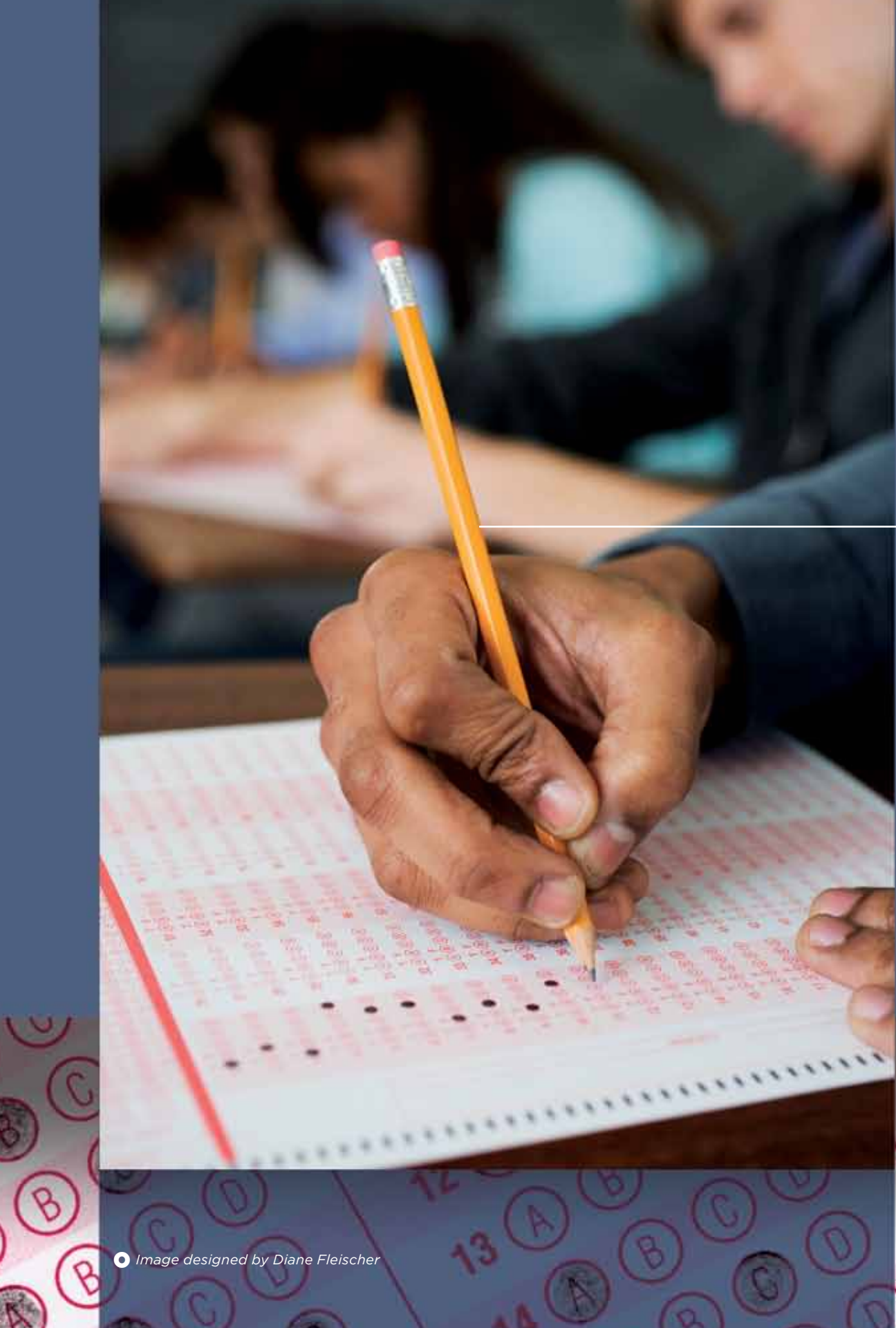


Image designed by Diane Fleischer

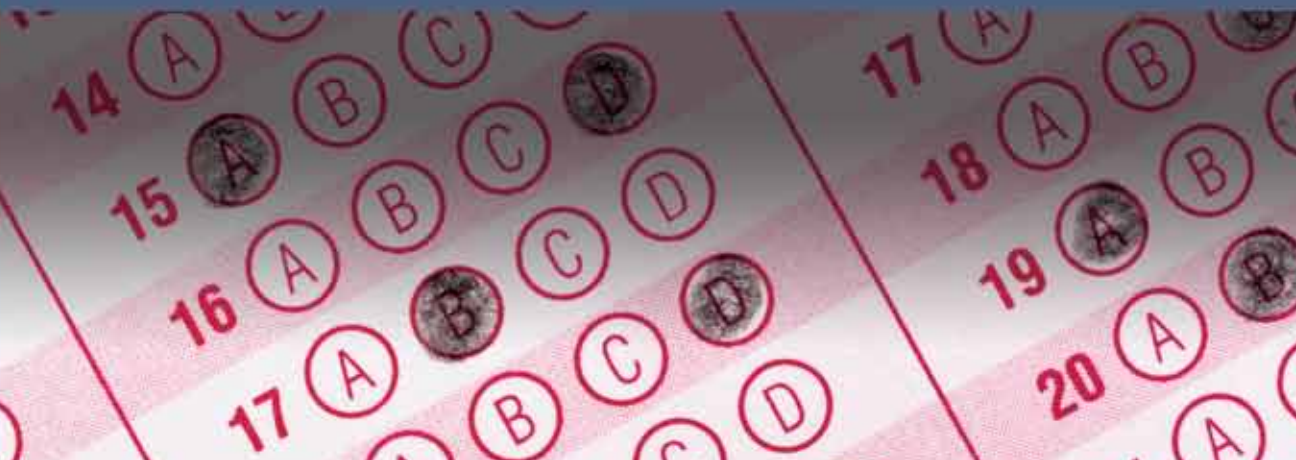
The Value of TRAINING: Analysis of DAU's Requirements Management Training

RESULTS

Charles M. Court, Gregory B. Prothero, and Roy L. Wood

In response to Congress, the Defense Acquisition University (DAU) designed and fielded a course of study for Requirements Management, including a 1-week advanced classroom course. While teaching this course, the DAU faculty routinely conducts pre-testing and post-testing to assist the faculty and students in assessing learning and retention. The faculty uses data from these tests, along with student demographics, to assess the value of learning the course provides and to explore some initial assumptions about the readiness of the workforce to learn. Results show a greater than 30 percent increase in learning from pre- to post-test and debunk nearly all the preconceived notions the university held about the incoming students.

Keywords: *student learning, student demographic, requirements management*



Every successful system acquisition begins with a well-thought-out set of operational capability requirements. The military services have always had some sort of requirements generation process that told the armories and shipyards what to build for the warfighter. As acquisition became more complex, expensive, and risky, the Department of Defense (DoD) recognized the need for a more formal system of articulating requirements and the importance of training both the acquisition and the requirements workforces.

The Joint Capabilities Integration and Development System

In 2003, then-Secretary of Defense Donald Rumsfeld initiated a formal DoD-level requirements generation process—the Joint Capabilities Integration and Development System (JCIDS). According to Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01H, "The JCIDS process exists to support JROC [Joint Requirements Oversight Council] and CJCS [Chairman of the Joint Chiefs of Staff] responsibilities in identifying, assessing, validating, and prioritizing joint military capability requirements" (CJCS, 2012). Within the context of the National Military Strategy, JCIDS provides a process to identify and assess the capabilities joint operational forces need to meet future military challenges. A capabilities-based assessment process identifies potential gaps in warfighting capability and drives changes to doctrine, organization, training, materiel, leadership and education, personnel, facilities, and/or policy (DOTmLPF-P). Many requirements lead to nonmateriel solutions, while other requirements call for materiel solutions. The JCIDS process generates the requirements and the associated performance criteria for those materiel solutions. The Defense Acquisition Management System then fulfills those requirements and delivers the required capabilities.

Articulating a new warfighting capability requirement and defending this need through rigorous discussion and analysis is a nontrivial undertaking for a requirements manager. A new military requirement can initiate a decades-long acquisition that requires the investment of billions of taxpayer dollars to develop, manufacture, and field. Requirements managers must be able to correctly identify, document, and support the compelling need for any new system, then be able to work alongside their

acquisition counterparts to field the new capability. This is a complex undertaking. In 2007, Congress formally directed the DoD to train the men and women who develop new requirements under JCIDS.

Requirements Management Training

The National Defense Authorization Act (NDAA) of 2007 mandated the Under Secretary of Defense for Acquisition, Technology, and Logistics (AT&L), in consultation with the Defense Acquisition University (DAU), to develop a training program to certify DoD personnel with the responsibility to generate capability requirements for major defense acquisition programs (NDAA, 2006). The congressional mandate called for training both military and DoD civilian managers charged with assessing, developing, validating, and prioritizing requirements through the JCIDS process. This broad definition covered relatively junior members of the workforce up to and including 4-star generals and admirals on the JROC who ultimately validate the requirements. This mandate created a need for a broad and diverse training program at several levels of sophistication. Further, as Court (2010) pointed out, "no one person does all four tasks of assessing, developing, validating, and prioritizing" requirements, so the training program would also need to address a wide variety of tasks and competencies.

DAU responded quickly to meet the congressionally imposed deadline to create and deploy a requirements management certification-training curriculum by September 30, 2008. Working with AT&L and the Joint Staff Directorate for Force Structure, Resources and Assessment (J8), DAU developed two online courses for requirements managers and a 1-day classroom workshop for general and flag officers. These courses were very successful, and by the end of fiscal year 2008, the community had logged more than 4,200 course completions. In 2010, DAU added a

TABLE 1. REQUIREMENTS MANAGEMENT TRAINING CURRICULUM

CLR 101 Introduction to JCIDS	RQM 110 Core Concepts for Requirements Management	RQM 310 Advanced Concepts and Skills	RQM 403 Requirements Executive Overview Workshop	RQM 413 Senior Leader Requirements Course
4–6 hours	24–30 hours	5 days	1 day	Tailored
A, B, C	B, C	C	D (1–3 Star/SES)	D (4-Star/Director of Agency)
Required Training Level Guidelines				
A	Contribute to the Requirements generation and capability development process in various capacities, including: JCIDS analysis, subject matter or domain expertise, document staffing and coordination and/or administrative support—***Requirements Originators and Support***			
B	Significantly involved with Requirements generation and capability development in specific capacities, i.e. study leadership, planning, writing, adjudicating comments, and facilitating inter-organizational development and coordination of Requirements documents—***Requirements Writers and Developers***			
C	Designated by organizational leadership for advanced Requirements instruction; Primary duties involve leadership/supervisory roles in requirements generation and capability development; Organizational representative in pertinent program management and JCIDS forums including FCB Working Group, FCB, JCB, and JROC meetings—***Requirements Supervisors, Presenters, and Trainers***			
D	GO/FO/SES—Validate and/or approve documents; provide senior leadership and oversight of JCIDS analysis and staffing: enforce Requirements standards and accountability—***Requirements Validators and Prioritizors***			

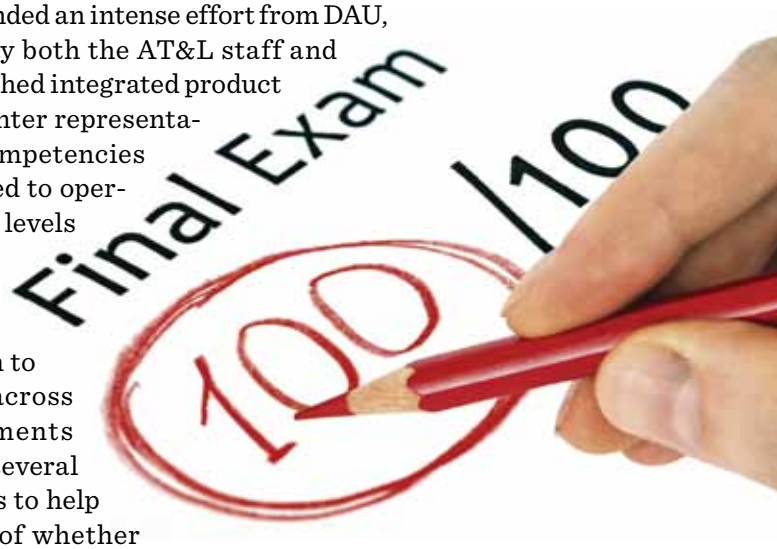
Note. SES = Senior Executive Service; FCB = Functional Capabilities Board; JCB = Joint Capabilities Board; GO/FO = General Officer/Flag Officer.

Source: Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS)

1-week Advanced Concepts and Skills for Requirements Management (RQM 310) classroom capstone course to the curriculum. Table 1 shows the requirements management curriculum for designated individuals as recently as 2014.

Requirements Management Training Curriculum

Developing new courses for requirements management was an entirely new area for DAU training outside the customary acquisition disciplines. The effort demanded an intense effort from DAU, supported and sponsored by both the AT&L staff and the Joint Staff. DAU established integrated product teams that included warfighter representatives to define the basic competencies requirements managers need to operate successfully at different levels of responsibility. The DAU faculty and outside subject matter experts meticulously developed instruction to meet these competencies across the spectrum of requirements tasks. The faculty adopted several innovative assessment tools to help DAU answer the question of whether or not the training, once deployed, would be effective.



Requirements Certification Capstone Course: New Beginnings and Opportunities

Developing RQM 310, the Advanced Concepts and Skills for Requirements Management course demanded an intense, months-long effort by requirements and acquisition experts to ensure the course conformed to the requirements management competency model and would challenge students to reach higher levels of understanding and performance. DAU designed and piloted the new 1-week course and rolled it out to students in 2010.

Creating an entirely new classroom course allowed DAU to test and apply many new concepts and technologies. RQM 310 includes faculty discussions, guest speakers, computer simulations, and a challenging student capstone exercise. One of the technology innovations in RQM 310 was the routine use of a classroom-participation system. With

this system, each student uses a response device that looks like a small remote control to respond to questions and assessments. During the first morning of the class, students use their response devices to take a course pre-test and review material from the course's online prerequisites. Throughout the week, students continue to use the response device to interact with faculty questions in the lessons. The RQM 310 students also use the response devices in an in-class simulation to evaluate and discuss differences between programs depending on their timeline, financial state, Service and Defense Agency priorities, and issues such as a budget breach or a failed operational test.

RQM 310 student demographics. Both military and civilian requirements managers attend RQM 310. Students come from the Pentagon as well as from far-flung Combatant Commands and field activities. Military members bring current and relevant experience to the requirements generation process. Typically, military requirements managers come from operational and warfighting specialties, and complete a requirements management tour between field assignments. However, there is a relatively high turnover of military personnel through requirements management positions, bringing in new personnel with limited to no JCIDS or acquisition experience, thus creating a steady demand for training. Civilian requirements managers have greater tenure in their positions, and provide continuity in requirements offices and a "corporate memory" for their organizations.

Assumptions about the workforce. Given the vastly different demographics of the workforce who attend RQM 310, initial expectations were that incoming knowledge and experience of the students might also be vastly different. For example, the DAU faculty assumed that civilian requirements managers, because of their longer tenure, would be better versed in JCIDS and acquisition procedures than their military counterparts. Another commonly held belief was that students working in the nation's capital or on a combatant commander's staff would be more knowledgeable coming into the course because of more direct involvement in generating and vetting requirements. In addition to assessing the overall value of training, this study tested these major assumptions about the workforce, and the results are presented later in this article.

Study Method

Participants

This study used the data the DAU faculty normally collects in the process of executing each RQM 310 class. For purposes of this study, the data collected were from the 2013 course offering. The faculty did not originally anticipate using this course pre-test data in a study, but rather as a review specifically to assist the students in identifying their own individual knowledge gaps, and to alert the faculty to particular areas of knowledge weakness in the class as a whole. Educational research has consistently shown that pre-testing can help increase student attentiveness during the course (Sadhasivam, 2013), and aid in focusing both students and faculty on improvement of particular knowledge gaps (Blin & Wilson, 1994; Wetstein, 1998).

While DAU developed the assessments and data collection primarily to improve learning outcomes, the data have been useful in providing valuable insights into other aspects of the training. The DAU faculty compares pre-test data to post-test data to determine overall student improvement and to assess the value of learning. Post-test data from the end-of-course assessment have similar, but not identical, questions as those on the pre-test. The faculty also analyzed pre-test data in this study against student demographics to determine whether one group might be better prepared for the advanced concepts course.

The DAU faculty compares pre-test data to post-test data to determine overall student improvement and to assess the value of learning.

Research Design

As noted earlier, this research used data collected from a total of 263 students during the normal execution of the RQM 310 course in 2013. The data collected include pre-test and end-of-course assessment scores collected with the student response system. Questions on the two tests are similar, but not identical, and both instruments focus on key learning and competencies needed by requirements managers to be effective in their jobs. All of the students attending the RQM 310 advanced course had previously completed the two online prerequisite courses: Introduction to the Joint Capabilities Integration and Development System (CLR 101), and Core Concepts for Requirements Management (RQM 110). These online courses are self-paced, computer-based training that include their own online assessments of student progress and understanding. RQM 110 classes have assigned faculty who are available to answer questions, mentor students who might be experiencing difficulty in the course, and otherwise provide academic or technical assistance the students might need.

DAU also collects student demographics in the RQM 310 class to help the faculty better appreciate the level of experience and exposure to identifying, assessing, and formulating capability requirements. Based on a priori assumptions mentioned earlier, the faculty collects student data on each student's assignment at the time he or she attended the course, their tenure in their current billet, aggregate experience working in the requirements management field, and how much of each student's day-to-day work content related to managing requirements. Table 2 shows a breakdown of the demographic questions and the granularity of the answers collected.

Analysis of Pre-Test and Post-Test Scores

As a first step in this analysis, tabulating and analyzing pre-test scores produced a mean score of 51.6 with standard deviation (s.d.) of 12.81. The tally of end-of-course scores showed substantial improvement with a mean of 80.97 and s.d. of 10.68. A paired-samples *t*-test showed the improvement in scores to be statistically significant, $t(262) = 37.173$, $p < 0.0005$. As noted earlier, many researchers—and faculty practitioners—recognize that pre-testing students can help focus their attention on desired outcomes and influence post-test outcomes. According to Kim and Wilson (2010), "there can be substantial effects of pretest on posttest, especially when the duration between them is short, that is, less than a month" (p. 755). Researchers must consider and compensate for

this fact in a strict research context. However, since the underlying purpose of the classes was to improve student knowledge and retention, the substantial improvement in scores was desirable regardless of the cause.

TABLE 2. STUDENT DEMOGRAPHIC CATEGORIES

Beltway?	Time in Billet	Experience	Percent Requirements Work	Career Field	Organization
Inside	0–6 Months	0–6 Months	0–25%	Require-ments	Joint Staff
Outside	6–12 Months	6–12 Months	25–50%	Operations	Service HQ Staff
	12–24 Months	1–3 Years	50–75%	Acquisition	Major Command
	> 24 Months	3–5 Years	75–100%	Other	Defense Agency
		> 5 Years	100%		OSD Staff
					Other

Analysis of the Student Demographics

As noted earlier, a number of assumptions about the student demographics produced expectations among faculty for those who might perform better in the class, and those who might require more assistance or remediation. During this research process, the DAU faculty wanted to test these assumptions statistically to determine their accuracy. To do so, the faculty tested each of the assumptions using SPSS *t*-tests or analysis of variation (ANOVA) to examine the mean scores of each subgroup on the pre-test data. The discussion below outlines the assumptions and test results. In short, almost none of the entering assumptions proved to be true, and the classes were far more homogeneous in terms of pre-test performance without regard to prior experience or assignment.

Assumption 1. Students from inside the (Washington, DC) Beltway would be better prepared than those in field activities outside the Beltway. An independent-samples *t*-test assessed the means of the pre-test scores between the two groups. The inside-the-Beltway group average pre-test score was 52.28 ± 12.5 and the outside-the-Beltway group posted an average score of 59.79 ± 13.2. The *t*-test analysis found no statistically significant differences between student groups at a 95% confidence level, $t(263) = 0.93$, $p = 0.473$.

Assumption 2. Students with more time in their current billet will be better prepared than those with shorter tenures. The assessment divided the students into those with less than 6 months in their current positions, those with 6–12 months, those with 12–24 months' tenure, and those with greater than 24 months in the job. Since many military requirements managers historically have shorter tours in requirements billets between operational tours, observers could assume that longer tenures might better prepare students for the advanced course. The analysis did not support this assumption, however. The means of the group scores on the pre-test varied only between 49.5 and 53.7. An ANOVA test on the groups revealed no statistically significant differences in their respective performances on the pre-test, $F(3, 258) = 1.11$, $p = 0.344$.

Assumption 3. Students with greater experience in requirements management would be better prepared. To test this assumption, the analysis subdivided the students into groups with less than 6 months' experience, those with 6–12 months' tenure, 1–3 years, 3–5 years, and greater than 5 years. An ANOVA test on this data did find a single statistically significant difference between groups of students as determined by the one-way ANOVA, $F(4, 258) = 3.096$, $p = 0.016$. A Tukey post-hoc test on the data revealed that students with 3–5 years of experience showed a statistically significant average higher score (56.7 versus 48.2) on the pre-test than less experienced students with 6–12 months' experience.

Assumption 4. Students who spend a greater amount of day-to-day time working on requirements will show better preparation for the class. For this test, the analysis divided the students into five groups: (1) students who reported working on requirements-related tasks less than 25% of the time; (2) those with requirements work between 25% and 50%; (3) students with requirements work from 50% to 75%; (4) those whose requirements content in their workday were between 75% and 100%; (5) students whose work was 100% exclusively related to requirements. The ANOVA analysis for these groups again pointed to no statistical differences between the pre-test means, $F(5,257) = 1.48$, $p = 0.195$. The pre-test average scores for these groups varied only between 50 and 53.6.

Assumption 5. Designated requirements managers, and perhaps acquisition professionals, will be better prepared for the class. Here, the demographic questions asked the students to self-identify their primary career field: requirements, acquisition, operational/warfighter, or other.

The ANOVA analysis of the mean pre-tests scores for these groups found no statistically significant differences, with mean scores between 48.9 and 53.6, $F(3, 259) = 0.880$, $p = 0.452$.

Assumption 6. Organizational assignment will have some impact on student readiness. The initial assumption was that there might be some relationship between the student's assigned organization and his or her score on the pre-test. For example, the faculty might expect a student assigned to the Joint Staff or Combatant Command to do more work

> ***This analysis debunked nearly every assumption about factors that might affect student preparedness for the advanced course.***

directly or indirectly in creating, assessing, or approving requirements than students from other organizations. For this analysis, the study broke the student sample into those who worked on the Joint Staff, Service Headquarters Staff, major military command, Defense Agency, Office of the Secretary of Defense Staff, a Combatant Commander Staff, or other. Once again, the ANOVA showed no statistical differences in mean pre-test scores of the students, regardless of their assignment, $F(6, 256) = 0.312$, $p = 0.930$.

Significance of the Analysis

This analysis debunked nearly every assumption about factors that might affect student preparedness for the advanced course. Each of these assumptions made sense on an intuitive level, and the results have been surprising. DAU will need to do more work to determine exactly why these assumptions were untrue, but preliminary analysis offers two potential explanations. First, the knowledge of students coming into the course is much more homogeneous than originally believed. This may be the result of all students being required to take the same online preparatory courses, Introduction to the Joint Capabilities Integration and Development System, CLR 101, and Core Concepts for Requirements

Management, RQM 110. Students who take these courses may come into the advanced RQM 310 with a common baseline of knowledge learned primarily from those classes. Another possibility is that individuals in the requirements community typically work only on single or perhaps a handful of tasks related to the broader process of identifying, assessing, validating, and prioritizing joint requirements. It is unlikely that any individual student would have a deep knowledge, based on experience, across the entire process, regardless of tenure or organizational assignment. Thus, expertise in any narrow area may not contribute to statistically higher scores on course material that covers all areas.

Summary and Conclusions

DAU responded to the congressional mandate and met the short deadline to train and certify requirements managers through a combination of online and classroom courses. The success of the initial DAU approach led to student demand and leadership support to expand the initial requirements curriculum. The most significant curriculum expansion was the development of the Advanced Concepts and Skills for Requirements Management course, RQM 310.

Developing a new classroom course in a different, nontraditional area of acquisition allowed the DAU faculty to apply new technologies. Classroom simulations enhanced traditional teaching approaches. The simulations encouraged the exchange of ideas. They helped requirements

> ***This analysis has also been a "myth buster" for a number of sincerely held assumptions about the workforce and how demographic factors influence RQM 310 student preparation.***

managers from different Services and Defense Agencies recognize their common problems. Classroom participation devices encouraged more student involvement.

The success of using classroom-participation devices led the requirements faculty to additional innovation. Students take a pre-test on the first day of class, and a final exam post-test at the end of the 1-week course. Both exams use classroom-participation "clickers" with the exam questions projected on a classroom screen. By comparing the results of the pre-test to the results of the post-test, this analysis has established that statistically significant improvements in scores occur, leading us to conclude with confidence that student learning was taking place.

This analysis has also been a "myth buster" for a number of sincerely held assumptions about the workforce and how demographic factors influence RQM 310 student preparation. Almost universally, the assumptions have been wrong, and students coming into the course are much more homogeneous than the faculty anticipated. Part of the homogeneity could result from all students taking the same prerequisite courses—CLR 101 and RQM 110—and coming into the advanced RQM 310 with a common baseline of knowledge learned from those classes. Another possibility is that individuals in the community work only on single or perhaps a handful of tasks related to identifying, assessing, validating, and prioritizing joint requirements, thus no individual student has a deep knowledge across the entire process, regardless of tenure or organizational assignment. Expertise in a narrow area may not contribute to statistically higher scores on course material that covers all areas.

Nevertheless, the success of pre- and post-testing in RQM 310 has encouraged the faculty to expand this approach to other requirements courses. Specifically, the faculty is investigating how to apply this approach to the online Core Concepts for Requirements Management course, RQM 110. Further, based on the success of RQM 310, additional classroom courses at the Defense Systems Management College have adopted the classroom simulations and the student-participation system, and are collecting student demographics and learning data to be able to continuously improve course content and learner performance.

Research Limitations and Future Research

As noted earlier, the data collected from the RQM students were primarily for the purpose of gauging the knowledge of the incoming students and ensuring that the course delivered important content in a way that was understandable and memorable. This analysis did not use random samples or experimental methods that would contribute to a rigorous scientific study. Future researchers may choose to close these obvious gaps in a more intentional way. In addition, post-testing performed at the end of the class does not guarantee the students will remember the information over the long term. Future research may wish to test students several weeks or months after graduation and assess the results of knowledge retention over time.

References

Blin, F., & Wilson, D. (1994). The use of pre-test and post-test in CALL {computer-aided language learning}: A case study. *Computers and Education*, 23(1), 143–150.

Chairman of the Joint Chiefs of Staff. (2012). *Joint capabilities integration and development system* (CJCSI 3170.01H). Washington, DC: Joint Chiefs of Staff.

Court, C. M. (2010). The manager in the muddy boots. *Defense AT&L Magazine*, 39(1), 12–16.

Kim, E. S., & Wilson, V. L. (2010). Evaluating pre-test effects in pre–post studies. *Educational and Psychological Measurement*, 70(5), 744–759. Retrieved from http://epm.sagepub.com/content/70/5/744

National Defense Authorization Act (NDAA) for Fiscal Year 2007, Pub. L. 109–364 § 801, 109th Cong. (2006).

Rumsfeld, D. (2003, October 31). *Initiation of a joint capabilities development process* [Memorandum]. Washington, DC: Office of the Secretary of Defense.

Sadhasivam, M. (2013). Introduction of pre-test and post-test enhances attentiveness to physiology lectures: Students' perceptions in an Indian medical college. *International Journal of Biomedical and Advance Research*, 4, 341–344.

Wetstein, M. E. (1998). Assessment of learning in the American government course: Results from a pre-test/post-test methodology. Presentation at the Annual Conference of the American Political Science Association, Boston, September 3–5.

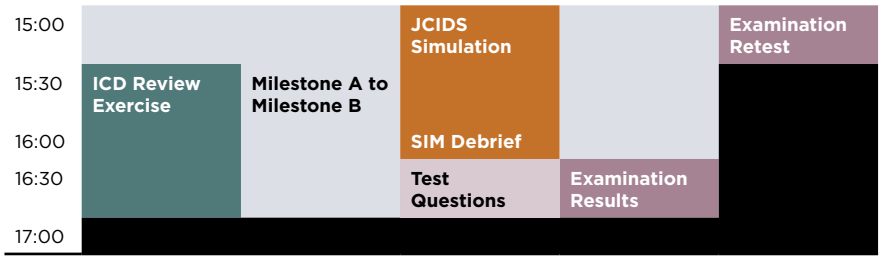
Appendix

The RQM 310 Class Schedule

Table A1 illustrates when the DAU faculty administers the pre-course assessment and the end-of-course examination. The table also lists the course topics and uses a color code to illustrate the different class activities. Table A2 explains the color code.

TABLE A1. RQM 310 DAILY CLASS SCHEDULE

	Monday	Tuesday	Wednesday	Thursday	Friday
8:00	Introduction and Orientation Class	AoA	Urgent Operational Needs	End of Course Examination	Capstone Exercise: FCB Briefing
8:30	Introductions and Teaming			External Influences—Guest Speaker	Outside Expert Evaluator
9:00	Pre-Course Assessment	MDD to Milestone A	DOTmLPF-P		
9:30					
10:00	RQM 110/ Game Show Review		Intel Support to Requirements	IT Documents Exercise	Guest Speaker—Expert Evaluator
					Capstone Exercise: FCB Staff
10:30		PPBE			
11:00	JCIDS and Acquisition		Milestone B to FOC	Prioritization Simulation	
11:30					Lunch
12:00	Lunch	Lunch	Lunch		
				Lunch	Capstone Exercise: FCB Staff ***
12:30					
13:00	Pre-MDD Analyses	Getting from AoA to KPPs	Test and Evaluation	DAU Knowledge Resources	Continuation ***
13:30	IS and IT Requirements Documents	KPP and KSA Development	CDDs	Capstone Introduction Capstone Briefing Preparation	
14:00			Writing Requirements		Course Wrap-up
14:30	ICD Review				



Note. AoA = Analysis of Alternatives; CDD = Capability Development Document; DOTmLPF-P = Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy; FCB = Functional Capabilities Board; FOC = Full Operational Capability; ICD = Initial Capabilities Document; IT = Information Technology; IS = Information System; JCIDS = Joint Capabilities Integration and Development System; KPP = Key Performance Parameter; KSA = Key System Attribute; MDD = Materiel Development Decision; PPBE = Planning, Programming, Budgeting, and Execution; RQM = Requirements; SIM = Simulation.

TABLE A2. COLOR CODES RELATING CLASS ACTIVITIES TO TOPICS IN TABLE A1
Administration
Examination or Examination Debrief
Lecture/Discussion
Guest Speaker
Exercise
Computer Simulation
Capstone Exercise Presentations
Course Wrap-up

Author Biographies

Dr. Charles M. Court is the Requirements Center director at the Defense Acquisition University. His career includes assignments as a Wild Weasel electronic warfare officer, a test realism manager, a program manager, and a laboratory supervisor. His teaching experience includes computer science, statistics, management, and physics. Dr. Court holds an MS in Physics from the Air Force Institute of Technology and a PhD in Management from Walden University. He holds Level III certifications in Program Management and in Systems Planning, Research, Development and Engineering.

(E-mail address: charles.court@dau.mil)

Mr. Gregory B. Prothero is the Requirements Center deputy director at the Defense Acquisition University and is the course manager for RQM 310, Advanced Concepts and Skills for Requirements Management. His military assignments include navigating operational C-130 missions, serving as Advance Agent for Air Force One, sponsoring Congressional travel as part of Air Force Legislative Liaison, and teaching as an assistant professor of Management at the United States Air Force Academy. He holds a Level C certification in Requirements Management and an MS in Operations Management from the University of Arkansas.

(E-mail address: gregory.prothero@dau.mil)

Dr. Roy L. Wood is the acting vice president of the Defense Acquisition University, and previously the dean of the Defense Systems Management College. He has served as the Principal Assistant Deputy Undersecretary of Defense for International Technology Security and as the director of the Militarily Critical Technologies Program. Dr. Wood holds an MS in Electrical Engineering from the Naval Postgraduate School, an MS in National Resource Strategy from the Industrial College of the Armed Forces, and a PhD in Organization and Management from Capella University.

(E-mail address: roy.wood@dau.mil)

INCREASE RETURN on Investment of Software Development Life Cycle by Managing the Risk

—A Case Study

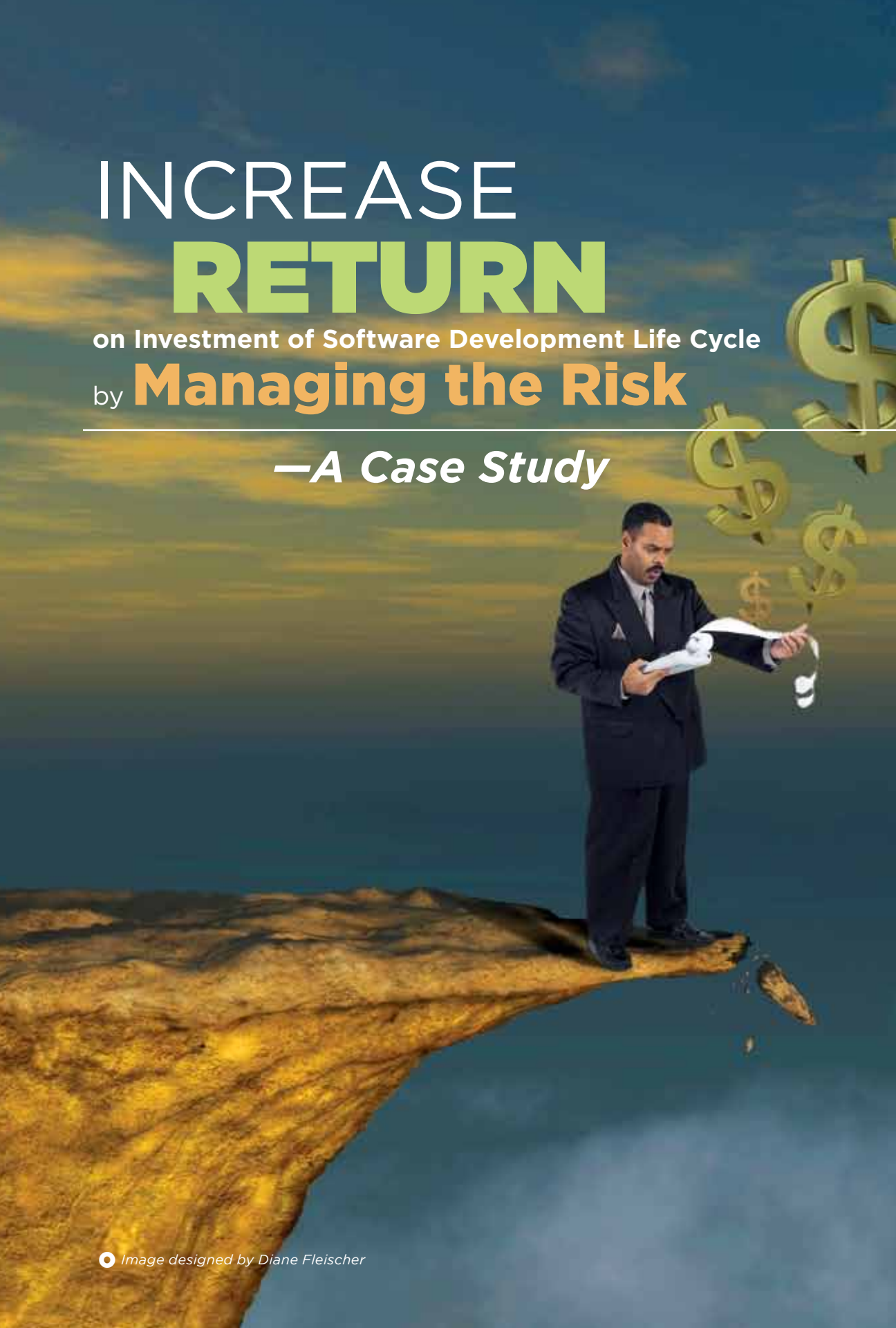


Image designed by Diane Fleischer

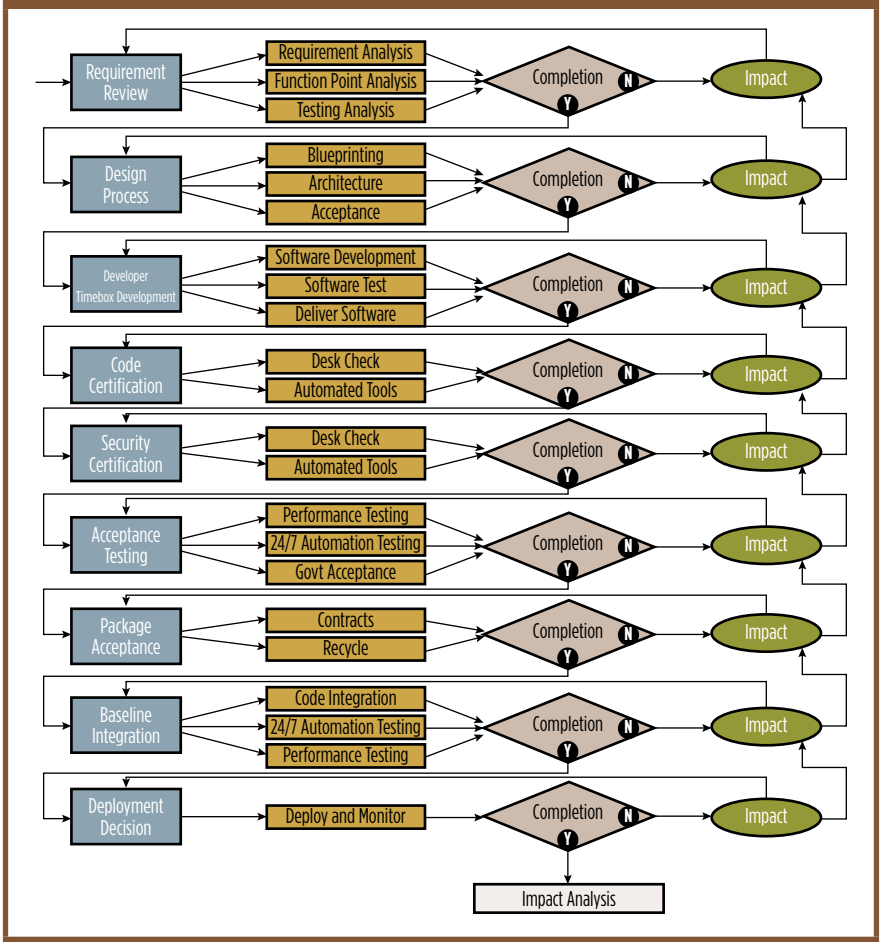
William F. Kramer, Mehmet Sahinoglu, and David Ang

This research article aims to identify and introduce cost-saving measures for increasing the return on investment during the Software Development Life Cycle (SDLC) through selected quantitative analyses employing both the Monte Carlo Simulation and Discrete Event Simulation approaches. Through the use of modeling and simulation, the authors develop quantitative analysis for discovering financial cost and impact when meeting future demands of an organization's SDLC management process associated with error rates. Though this sounds like an easy and open practice, it is uncommon for most competitors to provide empirical data outlining their error rates associated with each of the SDLC phases nor do they normally disclose the impact of such error rates on the overall development effort. The approach presented in this article is more plausible and scientific than the conventional wait-and-see, whatever-fate-may-bring approach with its accompanying unpleasant surprises, often resulting in wasted resources and time.

Keywords: *discrete event simulation (DES), Monte Carlo simulation (MCS), error or defect rate, return on investment (ROI), software development life cycle (SDLC)*

The science behind software development in metric terms of return on investment (ROI) is well known and taught by many. Much work has been accomplished in this area albeit lacking details of execution on a real-life problem (Ferreira, Collofello, Shunk, & Mackulak, 2009; Zhang, Kitchenham, & Pfahl, 2008; Zhang, Kitchenham, & Pfahl, 2010). The art of software development is a learned behavior and not one with which everyone becomes comfortable due to its intricacies and learning cycle. The same may be said with respect to software development life cycle (SDLC) management and distribution as depicted in Table 1, where the different phases of an SDLC process, when applied, provide specific inputs and expected outputs.

TABLE 1. LIFE CYCLE PHASE FLOW



Life Cycle Phase (Process) Flow

As with many processes, there is a beginning point and a delivery epoch. SDLC methodology is no different. It enables standardization for planning and organizing, and facilitates cost estimation. Though there are several different models available, many are tweaked to best fit the current process or a sequence of activities in a software development project. The life cycle used in this article (Table 1) has nine phases beginning with the requirement review and ending with the deployment decision. As one begins with the first phase (i.e., requirement review) and moves right, software developers will observe, at a minimum, the activities that must be performed in the phase (keep in mind this is a high-level depiction). Moving right, there is a decision to be made whether to proceed to the next phase or recycle back through the current phase for further refinement.

This decision is only one of many for the phases; however, it might be the most crucial. Not only will schedule and cost be impacted, but phase errors will drive substantial cost as well. An organization needs to understand the impact, and that is the intent of this article—namely to show the phase error impact to the SDLC, thereby reducing overall project management cost by improving the error rate.

Each phase will generate its own success criteria, allowing a development team to anticipate the degree of success that can be expected throughout the life cycle. Unfortunately, as a development team moves through the SDLC process, it is common to shift expected outputs to

the right and ultimately into the next phase, if only to remain on track regarding the end schedule or an expected financial burn rate. Ultimately, reality will set in and a price to be paid will become readily apparent, whether it be in the form of a scheduling or financial disruption.

This may be even more prevalent when it comes to the acquisition of custom software. To be better prepared for the impact of the shifting deliverables associated with the SDLC management process, one must understand the intricacies of the process and especially the impacts associated with a product that is either late or overbudgeted. Using a discrete event simulation (DES) and Monte Carlo simulation (MCS), as combined, may assist in quantifying a scenario impact. The primary raison d'etre of this article is to demonstrate the potential for modeling the SDLC management process and bring the cost-saving factor forward to improve the ROI by employing statistical simulation techniques. Therefore, the basis of this article is to bring attention to the use of modeling and simulation (M&S) in developing a quantitative analysis for discovering potential scheduling and financial ROIs within the parameters of meeting future demands of an organization's SDLC management process. More specifically, the potential impact is associated with errors accruing and accumulating throughout the process. That being said, one must be mindful that the methods used to compile this research article rely equally upon the art of simulation as well as the ever-enduring statistical and mathematical sciences behind the art of simulation. The statistical and mathematical computations used a significant amount of data gleaned from many years of software development experience. It is, however, through these years of experience with software development projects that we have come to appreciate an SDLC management process. Likewise, it is also during this process that we have learned to exercise

a degree of caution when evaluating those bidding to perform custom software development, who typically bid on the process with some degree of naiveté that views every requirement, algorithm, and interface as a nonissue and the work as always straightforward. Most of the time, this is not true, since hiccups invariably surface along the way, whether in the form of undefined requirements or bad test data. More often than not, unforeseen events occur, which ultimately impact both schedule and cost to the users' disadvantage.

Modeling and Simulation Methodology for a Case Study

To identify and incorporate software life-cycle phases along with function point analysis, software managers ought to associate the error rate per phase with the time distribution per phase. Organizations performing standard unit, integration, and functional testing will likely only remove approximately 70% of defects during the life-cycle phases (Jones, 2008). This practice will allow other defects to run through the life cycle until the bottleneck becomes apparent in the final testing phase. The model introduction takes this into account and assists with providing a rough order of magnitude (ROM) to the level of effort a program may encounter. In addition, the model also provides an alternative approach to facilitate ROMs with the appropriate schedule and additional resources.

Computer M&S, as programs or networks of computers mimicking the execution of an abstract model of many natural systems from physical and life sciences to social and managerial sciences, and primarily engineering, have become an integral part of digital experimentation. M&S proves useful to estimate the performance of complex engineering systems when too prohibitive for analytical solutions. A simulation is defined as the reproduction of an event with the use of scientific models. A model is a physical, mathematical, or other logical representation of a system, process, or phenomenon. Time-independent static MCS and, conversely, dynamic DES (to manage events in real time for engineering applications) have been extensively reviewed (Sahinoglu, 2013). Taxonomy-wise, simulated computer models may be stochastic or deterministic, and dynamic or static, and discrete or continuous. Computer simulation has been widely used in engineering systems to validate the

effectiveness of tentative decisions regarding a new plan or schedule, or its outcomes, without experiencing the actual conditions, which could cost more resources or partial to full destruction such as in the simulation of the nuclear bomb (Sahinoglu, 2007). In a book titled *Simulation Engineering* by Jim Ledin (2001), the author outlines his twofold purpose as follows:

> i) Simulation is an approach that can significantly accelerate the product development cycle and provide higher quality in the final system.
>
> ii) A simulation contains a set of mathematical models of one or more dynamic systems and the interactions between those systems and their environment. (p. 1)

Moreover, the Institute for Electrical and Electronics Engineers' *Spectrum* (June 2012) emphasized that the M&S effect is a creative and time-saving topic of interest relevant to automotive engineering of hybrid vehicles, finding solutions to treating nuclear waste, upgrading the nuts and bolts of the electrical power (Smart) grid, and supercomputing research, among other areas (Aoyama, 2012).

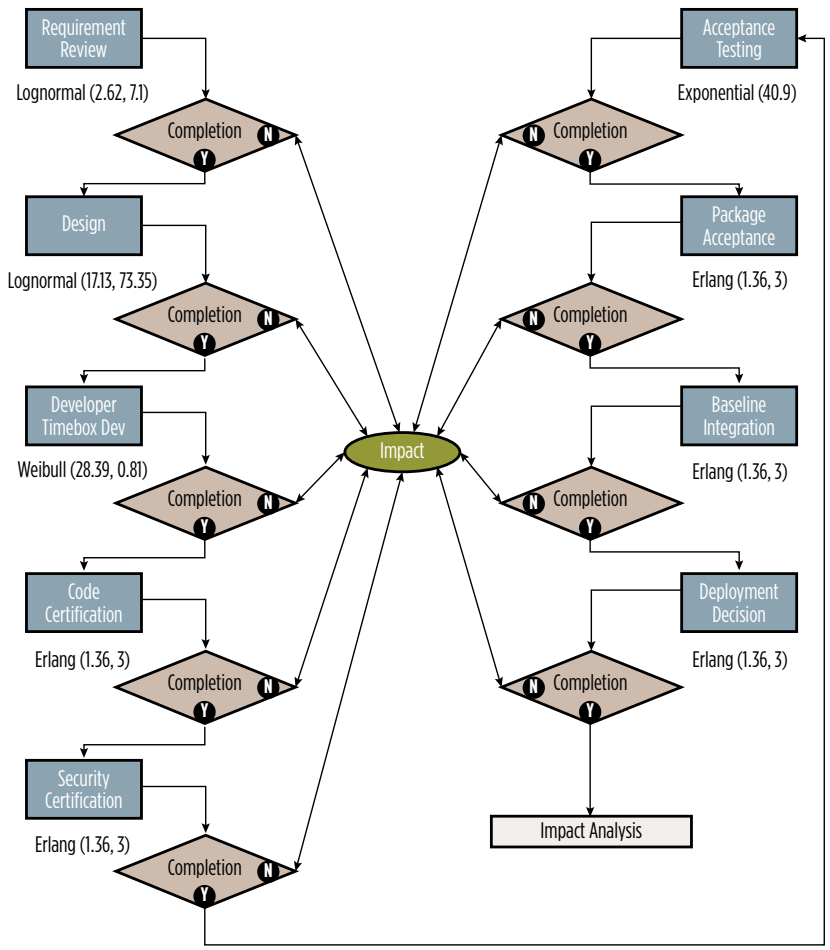
Simulation Approach

Table 2 depicts the conduct of an error rate analysis within the parameters of the SDLC management process. To better depict the probability distribution, Table 2 associates the probability distributions with each phase of the life cycle. Keeping in mind a waterfall model is in play, future research may requre further phase delineation among the many attributes of the phases. Note that:

- There is a need to simulate and model error rates within the SDLC process. Schedules and costs are impacted.
- Many models, such as waterfall, Agile, SCRUM, RAD, timebox, and spiral development methodologies exist today and could be used (Zhang, et al., 2010).
- This simulation model (Table 2) focuses on the error rates associated with waterfall methodologies.

- In order to determine cost per cycle and average cost per phase when using a development rate consisting of function point per staff month, calculate the error rates per phase and then aggregate with the suggested cost model.

TABLE 2. SOFTWARE DEVELOPMENT LIFE CYCLE DISTRIBUTION



Algorithmic Step-by-Step Approach Using Statistical Random Number Generation

Table 3 depicts iterations 1–1,000 and provides the details/samplings used in the simulation correlating the phases with probability distributions, the defect rates, repair rates, lambda, mu, standard deviation

TABLE 3. FACTS

	Per Function Point: 1						Utilization Factor: 0.8			
	Phase 1	**Phase 2**	**Phase 3**	**Phase 4**	**Phase 5**	**Phase 6**	**Phase 7**	**Phase 8**	**Phase 9**	
	Requirement Review	Design	Code Development	Code Certification	Security Certification	Acceptance Testing	Package Acceptance	Baseline Integration	Deployment Decision	
	Lognormal	Lognormal	Weibull	Erlang	Erlang	Exponential	Erlang	Erlang	Erlang	
	2.62, 7.1	17.13, 73.35	28.39, 0.81	1.36, 3	1.36, 3	40.9	1.36, 3	1.36, 3	1.36, 3	
Iteration										
1	0.3149	0.4046	0.6248	0.0024	0.0792	1	0.0027	0.0792	0.0697	
2	0.3417	0.4051	0.0091	0.1525	0.057	1	0.1333	0.0119	0.0712	
3	0.354	0.4076	0	0.1211	0.1406	1	0.0775	0.0266	0.0959	
4	0.3106	0.3994	0	0.151	0.0567	1	0.0382	0.081	0.0653	
5	0.3404	0.4035	0	0.0737	0.101	0.09998	0.0347	0.039	0.0178	
998	0.3452	0.3985	0.9986	0.1153	0.0296	1	0.0163	0.0309	0.0522	
999	0.35	0.4053	0.001	0.1401	0.0463	1	0.073	0.1473	0.0663	
1000	0.2606	0.4051	0	0.1321	0.0492	1	0.073	0.1473	0.0663	
Avg Defects Per Phase (Mean)	0.3086	0.4024	0.2259	0.0681	0.0697	0.9809	0.069	0.0687	0.0704	2.2636
Std Dev	0.0443	0.0052	0.395	0.0464	0.046	0.0946	0.0456	0.0464	0.0451	0.7686
Days Per Phase	25	20	80	10	15	10	5	10	5	180
Avg Defects Per Day	0.012344	0.020121	0.002824	0.006807	0.004644	0.098088	0.013802	0.006869	0.014071	0.179571
Avg Repairs Per Day	0.01543	0.025151	0.00353	0.008509	0.005805	0.12261	0.017253	0.008586	0.017589	0.224463
Defect % Per Day	6.874	11.2052	1.5727	3.7908						
Aggregate	Lambda	0.1796								
	Mu	0.2245								
	Beta	1								
	Mean	2.2636								
	Std Dev	0.7686								

(STD), and mean (Malone & Mizell, 2009). The average of the sampling was used along with a 180-day SDLC to determine defect rates per phase. These were used in the Java application to simulate and provide input to the findings in Table 4. Note the following:

TABLE 4. FINDINGS AND EXCEL SPREADSHEET RESULTS

SINGLE TEAM				TWO TEAM			
Phases	**Probability of Waiting**	**Days per Phase**	**Days to Repair**	**Phases**	**Probability of Waiting**	**Days per Phase**	**Days to Repair**
P1	0.76	25	18.94	P1	0.23	25	5.67
P2	0.8	20	16.04	P2	0.23	20	4.55
P3	0.8	80	64.696	P3	0.23	80	18.54
P4	0.8	10	8.016	P4	0.24	10	2.35
P5	0.79	15	11.91	P5	0.23	15	3.5
P6	0.77	10	7.698	P6	0.22	10	2.24
P7	0.83	5	4.148	P7	0.23	5	1.14
P8	0.83	10	8.348	P8	0.22	10	2.2
P9	0.81	5	4.027	P9	0.23	5	1.14
Summation	7.19	180	142.82		2.05	180	41.32
Average	0.8				0.23		
Hourly Rate		$55				$55	
Team Members		10				20	
Hours/Work Day		8				8	
C_H = Cost Hourly T_M = Average Development Team Size D_H = Work Hours per Day D_R = Repair Days TC = Total Cost				C_H = Cost Hourly T_M = Average Development Team Size D_H = Work Hours per Day D_R = Repair Days TC = Total Cost			
$TC' = (((D_R \cdot D_H) \cdot T_M) \cdot C_H)$				**$TC' = (((D_R \cdot D_H) \cdot T_M) \cdot C_H)$**			
Single Team Total Cost $628,421.20				**Two Team Total Cost $363,633.60**			
SAVINGS $264,787.60							

- Function point count is maintained at one function point for the life-cycle period of 180 days. With the distribution per phase identified along with the days per phase, the Average Defects per Phase (ADP) is introduced with the summation of the ADP to be the average defect per one function point.
- Next, the Average Defects per Day (ADD) is calculated by dividing the ADP by the Days per Phase. This output becomes our lambda (λ) in the phase calculation in determining our Probability of Waiting (PoW).
- The Average Repairs per Day (ARD) is determined by multiplying the ADD by our utilization factor of a constant 0.8 (80 percent) from best practices (Malone & Mizell, 2009). This output becomes our mu (μ), also used in determining the PoW.

Results

Factors used to obtain results (Table 3) follow:

- Average Defects per Phase = (summation of each phase distribution)/iterations
- Days per Phase = variable set by experience
- Average Defects per Day = (Average Defects per Phase)/(Days per Phase)
- Average Repairs per Day = (Average Defects per Day)/utilization factor.

To make use of the facts in Table 3, a Java application (see Appendix, Java Source Code First Page) was developed to conduct several thousand runs for the simulation and ultimately provide a statistical summary to support Excel findings. The facts from the spreadsheet shown in Table 4 were placed into this homebrewed java application where the user can identify the inputs, the number of runs, and lastly, can run with either a single-team or a two-team simulation.

Table 4 represents only one screen shot with a single distribution, while arbitrarily using cost per hour of $55, team size of 10, and work hours per day to equal 8. One can vary the cost factors. Taking these factors into account, the cost formula in Equation (1) is as follows:

Total Cost = (Days to repair • work hours per day • team size • hourly rate). (1)

We can begin to readily determine that the errors per phase quickly outpace the efforts of a single developer and throw the schedule and cost model far to the right. However, by adding a second development team to assist with the fixing of the errors per phase, the cost and schedule are only slightly impacted (Malone & Mizell, 2009).

One can better appreciate the long-term impacts when dealing with contracts and why the lower bid may initially seem the best value; however, with the software development life cycle, this may not be the case. Improper preliminary analysis and use of resources could easily whirl the schedule and cost into an embarrassing tailspin. The core of this research precludes this handicap.

Other findings and Excel spreadsheet results highlighted in Table 4 follow.

- PoW is multiplied with the Days per Phase to obtain the Days to Repair for each specific team.
- Multiple variables are added to obtain realistic cost of software development teams (such as hourly rate of developers, team size, and hours per workday).
- The formula used for each team is: Total Cost = (repair days • work hours • team size • hourly cost).

Validation

Does the lowest dollar contract actually deliver the best value? This is what the research confirms positively.

Verification

Validation of error rates and function point rates came from Jones (2008).

Outcomes

Development teams can determine cost at granular phases within the SDLC as it pertains to error rates within software development. Upon running the simulation, the aggregated results show significant financial benefits. Factors used to obtain results are shown in Table 3 (Malone & Mizell, 2009).

Conclusions

The article responds to the following question: When required to analyze best-value contracts without using a simulation model, does the requestor actually obtain true cost by analyzing a single entity to develop software versus aggregated cost (Table 4) delivered from an additional pool of resources? Future work along with inputs from software development cost models will go a long way in producing a better understanding of the true cost of software development and why there seems to be a schedule shift as the SDLC runs through its phases. This project scratches the surface by showing that the assumption by most software developers that all contracts and estimates provided are realistic, does not really portray the impact of errors to the schedules, which further increases cost. Some conclusive findings of interest are outlined below:

> ***If the errors are identified in the early stages of a software development acquisition, contracting officers may be in a better position to avoid the lowest contract bid if they understand where proper resources, when applied, may actually decrease cost and schedule, thus delivering a successful acquisition and software functionality.***

- Average cost per phase with single team to fix errors is an estimated $628,421.20 with the original summation of 180 days per phase.
- Adding an additional team to focus on errors, thereby increasing the cost for labor for two teams, equates to 42.14% savings. This is readily discerned in the reduced number of days to fix the errors. In fact, the second team will cost an estimated $363,633.60 in labor. The overall estimated savings is $264,787.60 for the cost of the repairs.
- Future and long-term analysis should focus on specific methodologies as well as on the coding language.

- Many organizations have invested in the use of the waterfall methodology and have been slow to appreciate the potential cost and schedule impact from error rates within the multiple phases of the SDLC.
- This article aimed to present a DES and MCS to determine an outcome that can be used to improve a process and cut costs. The error rate analysis project has done just that.
- Through lengthy discussions about rates within the MCS portion and the impact on business development systems, additional research and refinement may be sought to further develop the phase rates from within an organization. Additional research will provide better understanding of the impact for long-term software development and error rate impact.
- It is hoped that this and later work will enable future professionals in software development acquisition to establish a more definite cost analysis when confronting quantifiable data such as function points and development languages to give them a better understanding of the impact of development errors within the different phases of the waterfall SDLC.

An SDLC is a methodological process that from a high level can be used to determine schedules and costs and identify bottlenecks. However, it seems only recently that declining information technology budgets and increasing delivery costs require us to slice the life cycle into further granularity to understand better the cost and schedule impacts. In an attempt to correlate errors with phases and cost to fix, a prevailing assumption is that the cost of errors is flat. However, this may not be so. If the errors are identified in the early stages of a software development acquisition, contracting officers may be in a better position to avoid the lowest contract bid if they understand where proper resources, when applied, may actually decrease cost and schedule, thus delivering a successful acquisition and software functionality.

References

Aoyama, M. (2012). Computing for the next-generation automobile. *IEEE Computer*, 45(6), 32–37.

Ferreira, S., Collofello, J., Shunk, D., & Mackulak, G. (2009). Understanding the effects of requirements volatility in software engineering by using analytical modeling and software process simulation. *Journal of Systems and Software*, 82(10), 1568–1577.

Jones, C. (2008). *Applied software measurements: Global analysis of productivity and quality*. New York: McGraw-Hill.

Ledin, J. (2001). Simulation engineering—Build better embedded systems faster. Lawrence, KS: CMP Books.

Malone, L., & Mizell, C. (2009). Simulation model of spiral process. *International Journal of Software Engineering,* 2(2), 1–12.

Sahinoglu, M. (2007). *Trustworthy computing: Analytical and quantitative engineering evaluation*. Hoboken, NJ: Wiley & Sons.

Sahinoglu, M. (2013). Modeling and simulation in engineering. *Wiley Interdisciplinary Review Series (WIREs) Comput Stat 2013*, 5, 239–266.

Zhang, H., Kitchenham, B., & Pfahl, D. (2008). Reflections on 10 years of software process simulation modeling: A systematic review. Proceedings of International Conference on Software Process (ICSP 2008), *Lecture Notes in Computer Science* (Vol. 5007, pp. 345–356), Leipzig, Germany, May 10–11.

Zhang, H., Kitchenham, B., & Pfahl, D. (2010). Software process simulation modeling: An extended systematic review. Proceedings of International Conference on Software Process (ICSP 2010), *New Modeling Concepts for Today's Software Processes* (pp. 309–320), Paderborn, Germany, July 28–29.

Appendix

JAVA SOURCE CODE FIRST PAGE

```
//package negexp;
// W. Kramer

import java.awt.*;
import java.awt.event.*;
import javax.swing.*;
import java.util.Random;
import java.text.*;

public class NegExp extends JFrame {

//elements of user interface
   private JLabel trialsJLabel;
   private JLabel meanJLabel;
   private JLabel devJLabel;
   private JLabel MuJLabel;
   private JLabel BetaServiceJLabel;
   private JLabel errorRateJLabel;
   private JLabel LambdaJLabel;
   private JLabel BetaJLabel;
   private JLabel servTimeJLabel; //package negexp;
// W. Kramer

import java.awt.*;
import java.awt.event.*;
import javax.swing.*;
import java.util.Random;
import java.text.*;

public class NegExp extends JFrame {
```

Author Biographies

Mr. William F. Kramer has over 25 years in the Information Technology field. He has developed, sustained, and operated military information systems. His experience includes application design, development, software life-cycle management, and systems engineering. His education includes a BS in Computer Science from Chapman University, an MS in Management Science from Faulkner University, and an MS in Cybersystems and Information Security from Auburn University at Montgomery. Mr. Kramer is retired from the U.S. Air Force, with 20 years' active duty. He is currently employed with the U.S. Air Force as a federal civilian.

(E-mail address: wkramer@aum.edu)

Dr. Mehmet Sahinoglu is the founder/director of the Informatics Institute, and the Cybersystems and Information Security (CSIS) graduate program at Auburn University in Montgomery. As an Institute of Electrical and Electronics Engineers senior member and a Fellow of the IEEE Signal Processing Society, he authored 120 conference proceedings, 50 journal articles, *Trustworthy Computing* by Wiley (2007), *Cyber-Risk Informatics* by Wiley (2015), and managed 15 grants. Dr. Sahinoglu holds a PhD from Texas A&M and an MS from University of Manchester Institute of Science and Technology in Electrical and Computer Engineering, respectively.

(E-mail address: mesa@aum.edu)

Dr. David Ang is an industrialist and a business professor, with 20-plus years of experience in many facets of business from both a pragmatic perspective and real-life applications. He has published more than 70 articles in academic business research journals and conference proceedings. Dr. Ang holds a PhD in Industrial Management and Systems Engineering from the University of Alabama in Huntsville.

(E-mail address: dang@aum.edu)

Manage TOWARD SUCCESS

—Utilization of Analytics in Acquisition Decision Making

Sean Tzeng and K. C. Chang

Large information technology (IT) projects such as Defense Business System (DBS) acquisitions have been experiencing an alarming rate of large cost overruns, long schedule delays, and under-delivery of specified capabilities. There are strict defense acquisition laws/regulations/policies/guidance with an abundance of review and oversights, generating a plethora of data and evidence for project progress. However, with the size and complexity of these large IT projects and sheer amount of project data they produce, there are challenges in collectively discerning these data and making successful decisions based on them. This research article develops an analytic model with Bayesian networks to orient the vast number of acquisition data and evidence to support decision making, known as the DBS Acquisition Probability of Success (DAPS) model.

Keywords: *defense business system, acquisition, analytics, evidential reasoning, Bayesian networks*

Image designed by Diane Fleischer

Developing an information technology (IT) system to meet organizational needs is not a simple task. It is often very extensive, taking a long time to realize, and more costly and difficult than originally imagined. This is especially true for large IT projects (over $15 million). In a 2012 study, University of Oxford researchers reported that, on average, large IT projects run (based on 5,400 IT projects) 45% over budget, 7% over time, and are delivered with 56% less value (Bloch, Blumberg, & Laartz, 2012). The situation seems to be even worse for Department of Defense Business System (DBS) acquisition programs, where the majority of programs would meet the University of Oxford researchers' threshold for large IT projects. A Government Accountability Office (GAO, 2012) report indicates that of 10 Enterprise Resource Planning programs the Department of Defense (DoD) identified as critical to business operations transformation, nine of the programs were experiencing schedule delays up to 6 years, and seven of the programs were facing estimated cost increases up to or even over $2 billion. This is occurring even though acquisition laws, regulations, policies, guidance, independent assessments, technical reviews, and milestone reviews guide DBS acquisition.

Great amounts of data and a large number of artifacts are generated during execution of DBS programs. A few examples include the Integrated Master Schedule (IMS), Earned Value Management System (EVMS) Metrics, Business Case, and Systems Engineering Plan (SEP), as well as Risk Reports and various independent assessments. These data/artifacts are commonly used by decision makers at technical reviews and milestone reviews as evidence of program progress to support their decisions. However, the development and use of evidence to support decisions has not translated to desirable investment outcomes. This issue is analogous to the experience of other professional disciplines such as intelligence, criminal justice, engineering, and medical professions. In today's Information Age, acquisition and availability of information and evidence no longer represent the most

challenging issues. Often data/evidence is abundant, but the availability of analytical tools limits the ability to figure out what all the evidence means collectively and how it supports the hypothesis being sought. Good decision making requires not only information and evidence, but the inference and representation of the evidence to support decision making. Currently, DBS acquisition decision makers have limited means to aid them in holistically and logically processing what all the available evidence collectively indicates about a program, and for using that evidence in a structured manner to support decision making.

DBS Acquisition Probability of Success (DAPS) is the evidence-based analytical tool developed to help decision makers collectively draw inferences from the abundance of available evidence produced during the course of DBS acquisition. Based on observations and inferences of evidence, the DAPS model is able to assess program performance in specific subject matter knowledge areas and assess the overall likelihood for program success. DAPS is a way ahead to support acquisition decision making, and an initial step forward in improving human understanding and ability to innovate and engineer systems though evidential reasoning.

Theoretical Foundations

A brief discussion on the theoretical foundations behind the DAPS research is presented in this section. Topics include evidential reasoning and knowledge-based management.

Evidential Reasoning

According to Schum (2001), evidence is described as "a ground for belief; testimony or fact tending to prove or disprove any conclusion" (p. 12). The evidence within the framework of a DBS acquisition program includes the artifacts, technical plans, facts, data, and expert assessments that will tend to support or refute the hypothesis of program success. However, evidence by nature is incomplete, inconclusive, ambiguous, dissonant, unreliable, and often conflicting (Schum, 2001), making the decision process based on the observations and inferences of evidence a challenging and difficult endeavor. Evidential reasoning utilizes inference networks to build an argument from the observable evidence items to the hypothesis being sought. In the case of DBS acquisition, the DAPS model argues for the hypothesis of program success or the alternative hypothesis of program failure based on the observations of evidence.

A Bayesian network is a graphic modeling language used in this research to build the inference network for evidential reasoning. Its basis is the Bayesian approach of probability and statistics, which views inference as belief dynamics and uses probability to quantify rational degrees of belief. Bayesian networks are direct acyclic graphs that contain nodes representing hypotheses, arcs representing direct dependency relationships among hypotheses, and conditional probabilities that encode the inferential force of the dependency relationship (Neapolitan, 2003).

A Bayesian network is a natural representation of causal-influence relationships (CIRs), the type of direct dependency relationships built in the DAPS model. CIRs are relationships between an event (the cause) and a second event (the effect), where the second event is understood as a consequence of the first. CIRs are an important concept of Bayesian networks, and reflect stronger bonds than dependency relationships, which are not causal-based (Pearl, 1988).

Knowledge-based Management

The DAPS model framework is based on the concept of knowledge-based acquisition described by the GAO. In the GAO (2005) report for National Aeronautics and Space Administration (NASA) acquisition programs, GAO recommended to NASA, and NASA subsequently concurred, that transition to a knowledge-based acquisition framework will improve acquisition program performance. The GAO has also made the same recommendation to the DoD in other GAO reports, including the GAO (2011) report.

GAO (2005) describes the knowledge-based acquisition as follows:

> A knowledge-based approach to product development efforts enables developers to be reasonably certain, at critical junctures or "knowledge points" in the acquisition life cycle, that their products are more likely to meet established cost, schedule, and performance baselines and, therefore provides them with information needed to make sound investment decisions. (p. 9)

The more knowledge is achieved, the less risk or uncertainty the program is likely to encounter during the acquisition process. Sufficient knowledge reduces the risk associated with the acquisition program and provides decision makers and program managers higher degrees of

certainty to make better decisions. The concept of the knowledge-based acquisition is adapted in this research and built into the DAPS model. The Knowledge Points mentioned in the *Defense Acquisition Guidance* and the GAO reports are called Knowledge Checkpoints in the DAPS model. DAPS also contains Knowledge Areas, which are the subject matter areas of DBS acquisition in the model, derived from Project Management Institute (PMI)'s (2008) Knowledge Areas.

DAPS Bayesian Network Model

DAPS is developed with a Bayesian network model in the Netica software tool (Norsys, 2010). By using a Bayesian network, DAPS was able to construct a complex inference network to measure the certainties/uncertainties in subject matter Knowledge Areas and assess the level of success achieved at Knowledge Checkpoints.

Model Topology

The DAPS Bayesian network model contains a three-level structure, representing the three types of nodes in the model. Three types of static arcs also represent the interrelationships among the three types of nodes at a point in time, and one type of dynamic arc represents the temporal relationships from one point in time to another. The DAPS model at the first Knowledge Checkpoint, Material Development Decision (MDD), is shown in Figure 1. The topology of the top two levels—Knowledge Checkpoint and Knowledge Areas—is repeated at each of the 15 Knowledge Checkpoints. The bottom level containing the Evidence Nodes—the observation points of the DAPS model—varies at each Knowledge Checkpoint, depending on various evidence requirements.

FIGURE 1. DAPS MODEL AT MATERIAL DEVELOPMENT DECISION KNOWLEDGE CHECKPOINT

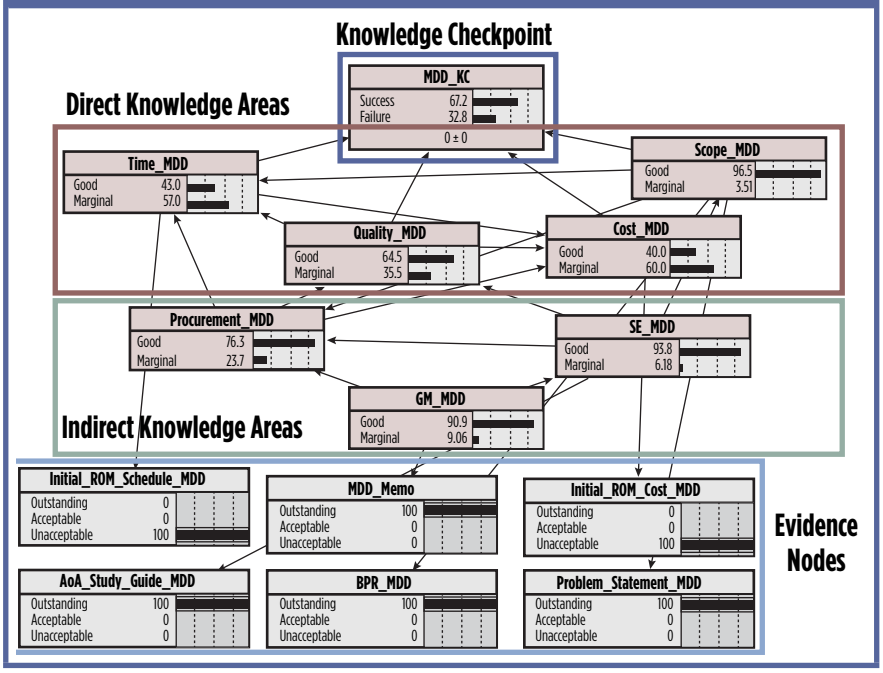


Table 1 outlines these DAPS model elements.

The complete DAPS model contains 15 Knowledge Checkpoints. Each Knowledge Checkpoint has one Knowledge Checkpoint Node, seven Knowledge Area Nodes, and a number of Evidence Nodes. The total is:

- 15 Knowledge Checkpoint Nodes
- 105 Knowledge Area Nodes
- 258 Evidence Nodes
- 258 KA2E Arcs
- 195 KA2KA Arcs
- 60 KA2KC Arcs
- 98 KA2KAi+1 Arcs

TABLE 1. DEFENSE BUSINESS SYSTEM ACQUISITION PROBABILITY OF SUCCESS (DAPS) ELEMENTS	
Nodes	• Knowledge Checkpoint Nodes (KC) • Knowledge Area Nodes (KA) • Evidence Nodes (E)
Static Arcs	• Knowledge Area Node to Knowledge Checkpoint Node Arcs (KA2KC) • Knowledge Area Node to Knowledge Area Node Static Arcs (KA2KA)
Dynamic Arc	• Prior Knowledge Area Node at the previous Knowledge Checkpoint to the same Knowledge Area Node at the next Knowledge Checkpoint Dynamic Arcs (KA2KAi+1)

Knowledge Checkpoint Node. The Knowledge Checkpoint is the top-level node, which cumulates all information about the DBS acquisition program at that decision point, assessing the likelihood of program success. It provides a cumulative measurement of success achieved by the program up to the current Knowledge Checkpoint, and is the metric that can be used to help decision makers decide whether the program has demonstrated enough certainty and maturity to move on to the next phase.

Knowledge Checkpoints are modeled as leaf nodes. They have no children nodes and contain four Knowledge Area Nodes as parent nodes: time, quality, cost, and scope Knowledge Area Nodes, which are the four measurable (direct) Knowledge Areas in the DAPS model. These CIRs on the Knowledge Checkpoint Node represent the four direct measures of success. Success is defined in DAPS as meeting program time, cost, and quality goals from a clearly defined program scope. The Knowledge Area Nodes are further discussed in the next section. Table 2 lists the 15 technical reviews and milestone reviews modeled in DAPS as Knowledge Checkpoints (Defense Acquisition University, 2013).

Knowledge Checkpoint Nodes contain two states describing the state of the program: "Success" and "Failure." The probability of these states reflects the knowledge (certainty) and risk (uncertainty) assessment of the program at the Knowledge Checkpoint.

Knowledge Area Node. Knowledge Areas are the second-level node, which measures the certainty and maturity attained for that particular subject matter area of DBS acquisition at the Knowledge Checkpoint. Knowledge Areas in DAPS are derived from the nine Project

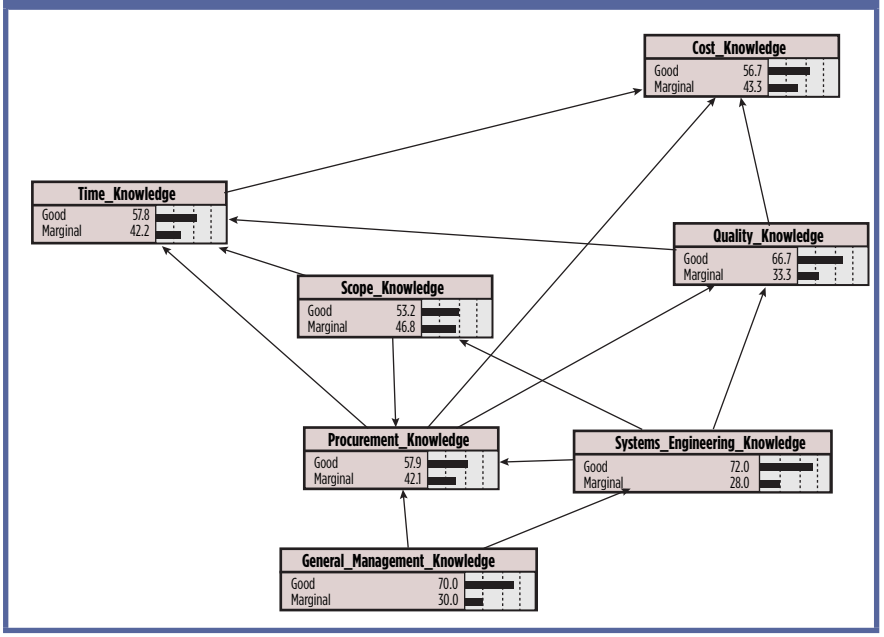
Management Body of Knowledge (PMBOK) Knowledge Areas (Project Management Institute, 2008), integrated with the systems engineering elements of defense acquisition. These Knowledge Areas are further divided into the measurable (direct) and enabling (indirect) Knowledge Areas. Measurable Knowledge Areas include scope, cost, time, and quality subject matter areas, which directly affect the measures of program success in DAPS. Enabling Knowledge Areas include general management, systems engineering, and procurement subject areas, which do not directly affect the measure of program success, but are important enabling factors that drive success.

TABLE 2. CASE 1 DAPS MODEL OUTPUT

KC	P(Success)	Success Factor
MDD	67.4	2.067484663
ITR	67.1	2.039513678
ASR	64.5	1.816901408
MSA	55.8	1.262443439
SRR	56.3	1.288329519
SFR	56.9	1.320185615
PreED	56.4	1.293577982
MSB	55.2	1.232142857
PDR	53.9	1.169197397
CDR	52.8	1.118644068
TRR	51.9	1.079002079
MSC	51.2	1.049180328
PRR	50.8	1.032520325
IOC	50.5	1.02020202
FOC	50.3	1.012072435

The Knowledge Areas represent an important aspect of the DAPS model. They model the static and dynamic complex interrelationships and effects within DBS acquisition and combine the observations of various evidence items in the subject matter Knowledge Area. The arcs among the Knowledge Area Nodes at a static point—the KA2KA arcs—model the CIR of how knowledge in one Knowledge Area affects knowledge in the second Knowledge Area. The KA2KA relationships in DAPS are shown in Figure 2, which is extracted from the model structure presented in Figure 1. The arcs in the KA2KA structure are selected based on the expert knowledge elicitation conducted as part of this research.

FIGURE 2. KNOWLEDGE AREA TO KNOWLEDGE AREA (KA2KA) GRAPH STRUCTURE

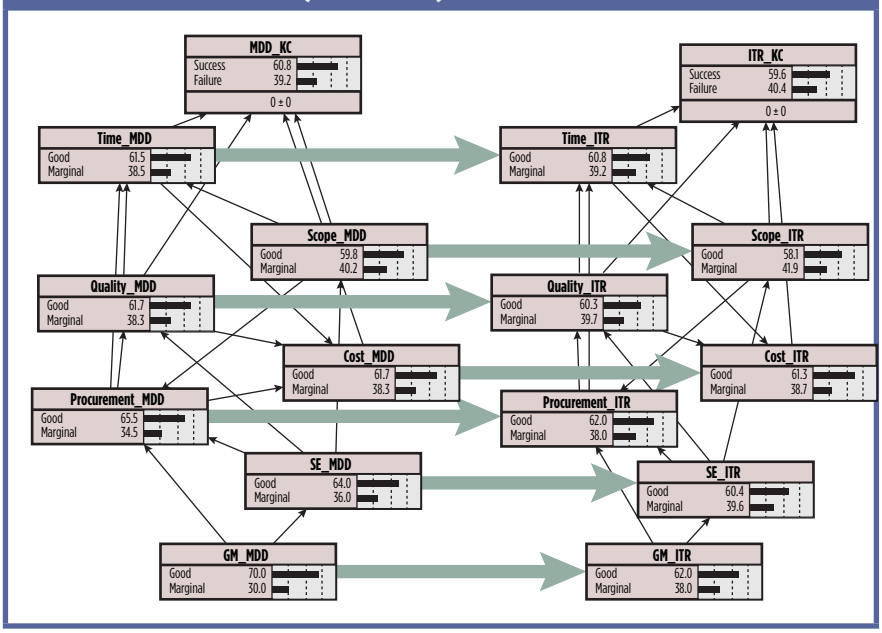


The dynamic arcs from a Knowledge Area Node at the prior Knowledge Checkpoint to the same Knowledge Area Node at the next Knowledge Checkpoint—the KA2KAi+1 arcs—model the CIRs of DBS acquisition through time. The KA2KAi+1 arc represents the knowledge in a Knowledge Area at a prior Checkpoint influencing the knowledge of the same Knowledge Area at the next Checkpoint. DAPS uses Knowledge Area Nodes to model the dynamic effects in the progression of knowledge during an acquisition project. Thus, each Knowledge Area Node gains information from the observations at the current Knowledge Checkpoint, as well as the information cumulated from prior Knowledge Checkpoints.

Figure 3 provides an example graph of the KA2KAi+1 arcs in green arrows from the MDD Knowledge Checkpoint to the next Initial Technical Review Knowledge Checkpoint.

The arcs from Knowledge Area Nodes to Evidence Nodes—the KA2E arcs—model the CIR of how knowledge affects the outcome observed with the evidence. Figure 4 provides an outline of the seven Knowledge Areas and select samples of the evidence grouped under each Knowledge Area.

FIGURE 3. KNOWLEDGE AREA @ KC1 TO KNOWLEDGE AREA @ KC2 (KA2KAi+1) ARC EXAMPLE



Knowledge Area Nodes contain two states describing the state of the knowledge level achieved in the subject matter Knowledge Area: "Good" and "Marginal." The probabilities of these states reflect the knowledge (certainty) and risk (uncertainty) in the subject matter Knowledge Area.

Evidence Node. The third- and bottom-level nodes are the Evidence Nodes in the DAPS model. Observations of Evidence Nodes are entered at this level to drive inference for assessing a program's probability of success. The only CIRs for this level are the arcs from Knowledge Area nodes to Evidence Nodes—the KA2E arcs described previously.

Evidence Nodes contain three states describing the state of the evidence: "Outstanding," "Acceptable," or "Unacceptable." In summary, these states reflect the risk assessment of the program in the specific Knowledge Area. Outstanding would require no worse than a "Low-Risk" assessment. Acceptable would require no worse than a "Moderate-Risk" assessment. Unacceptable would require a "High-Risk" assessment or worse. Since these are the Evidence Node observations, one of the states is chosen to describe the real-world observation of the evidence. This provides information to the parent Knowledge Area Nodes, which updates the belief in the Knowledge Area.

FIGURE 4. SAMPLE OF EVIDENCE TAXONOMY BY KNOWLEDGE AREA

ENABLING (INDIRECT) Knowledge Areas			MEASURABLE (DIRECT) Knowledge Areas			
General Management	**Systems Engineering**	**Procurement**	**Scope**	**Cost**	**Time**	**Quality**
Personnel/Staffing	AoA	Acquisition Plan	System Architecture	CARD/BOM/ ItemList	POA&M	CDRL Inspect/ Accept
Business Case/ Problem Statement	Market Research	Acquisition Strategy	DoDAF Architecture Data	Program Cost Estimate	Program Schedule Progress	Product Inspect/Accept
Program Charter	Systems Engineering Plan	RFP	Functional Baseline (Functional Requirements)	Independent Government Cost Estimate	EVMS—Time	Test Report (contractor), sub-level, integration
Program Budgeting and Funding	Test and Evaluation Strategy/Plan	Source Selection Plan	Allocated Baseline—System Requirements	EVMS—Cost	Time Elapsed	Test Report (GOV)—Verification, Validation and Acceptance
CAE Memo	Life Cycle Sustainment Plan	Vendor Questions	Allocated Baseline—Interface Requirements	Expenditure	Time Risk Report/ Independent ERAM	Defect Report/ Defect Rate
Program Certification	Project Management Plan/Software Development Plan	SSEB Report	Acquisition Program Baseline	Cost Risk Report/ Independent ERAM		DAICAP Authority to Operate Status
Acquisition Decision Memorandum	Risk Management Plan	SSAC Report	Product Baseline—System Design Document			Program Protection Plan
Material Development Decision Memorandum	Technical Review Reports	CPARS	Detailed Interface Description			Prototype Performance
Investment Decision Memorandum		SSA Selection Justification	Information Support Plan			Independent Logistics Assessment
			Test Cases			Independent Testing Assessment

Note. CARD = Cost Analysis Requirements Description; BOM = Bill of Materials; CAE = Component Acquisition Executive; CDRL = Contract Data Requirements List; CPARS = Contractor Performance Assessment Reporting System; DoDAF = Department of Defense Architecture Framework; DIACAP = DoD Information Assurance Certification and Accreditation Process; ERAM = Enterprise Risk Assessment Manager; EVMS = Earned Value Management System; GOV = Government; POA&M = Plan of Action and Milestones; RFP = Request for Proposal; SSAC = Security and Stability Advisory Committee; SSEB = Source Selection Evaluation Board.

Model Summary

To summarize the model, Figure 1 shows the inference network at one static point. At this point, Evidence Nodes are observed in accordance with the three node states (Outstanding, Acceptable, or Unacceptable) to provide information on the assessment of the certainty/maturity in the seven Knowledge Area Nodes through the KA2E arcs. The assessments are evaluated according to the two Knowledge Area Node states: Good and Marginal. The Knowledge Area Nodes then propagate the information according to the KA2KA arcs to combine the belief, based on the evidence observed under the Knowledge Area, as well as the belief in other Knowledge Areas where a CIR relationship exists. Finally, the Direct Knowledge Area Nodes provide information to the Knowledge Checkpoint Node to assess the belief in the Knowledge Checkpoint Node states—Success and Failure—through the KA2KC arcs, which completes the information flow within a static point at a Knowledge Checkpoint.

> ***Measurable Knowledge Areas include scope, cost, time, and quality subject matter areas, which directly affect the measures of program success in DAPS.***

The information at the static point within a Knowledge Checkpoint is then passed on to the next Knowledge Checkpoint using the seven Knowledge Area Nodes through the KA2KAi+1 arcs, where Evidence Node assessment observations will again be made. The information flow process is then repeated 14 times until the last Knowledge Checkpoint Node—the Full Operating Capability (FOC) Knowledge Checkpoint Node—is propagated.

DAPS Decision Process and Case Analysis

DAPS is an analytic model that assesses program performance in subject matter Knowledge Areas and measures the overall likelihood for success. Its basis is the observations of evidence already being conducted through acquisition reviews and oversight. DAPS has significant potential to aid decision makers in holistically and logically processing the mountain of evidence to support their acquisition decision making at Knowledge Checkpoints. This section will first discuss how DAPS could be used in the acquisition process and then demonstrate its use through a case analysis and associated what-if analysis.

DAPS Support of Acquisition Process

The highest level of DAPS model output is the probability of success measurements at the Knowledge Checkpoint Nodes, based on the program knowledge (certainty) level attained. This highest level DAPS model output is the cumulative metric to support decision making at Knowledge Checkpoints, aided by the measurements at the second-level Knowledge Area Nodes.

Three alternative views are available to the decision maker to observe this top-level output of DAPS.

$$\text{Success Factor} = \frac{P(KC = \text{Success})}{P(KC = \text{Failure})} \qquad (1)$$

First is simply the probability of success at the Knowledge Checkpoint, P(KC = Success), as outputted from the DAPS model.

The second alternative view is the translation of the probability of success at Knowledge Checkpoint Nodes into a "Success Factor"—the likelihood ratio of Success over Failure. This view intends to help decision makers better comprehend the chance for success in terms of ratios, illustrating the odds the program is more likely to succeed than fail, shown in Equation (1).

The success factor is presented in a format similar to the safety factor, which is commonly used in engineering applications as a simple metric to determine the adequacy of a system, as well as the widely used EVMS metrics of the Cost Performance Index and Schedule Performance Index.

A success factor above 1 indicates that the program is more likely to succeed than fail, while a success factor below 1 indicates that the program is less likely to succeed than fail.

The third alternative view is by the use of adjectival ratings (DoD, 2011) to describe the Knowledge Checkpoint assessment level. Table 3 provides the range of success factors used for the case analysis, their respective P(KC = Success) ranges, their associated adjectival ratings and risk levels, as well as the prescriptive recommended decisions for the respective range and rating. The ranges and ratings recommended in Table 3 reflect a risk attitude based on heuristics drawn from safety factor applications. Each organization or decision maker would be able to change the ranges and associated ratings based on their own risk attitude.

TABLE 3. KNOWLEDGE CHECKPOINT ASSESSMENT AND DECISION GUIDE

Success Factor	P(KC=Success)	KC Assessment Level	Recommended Decision
>9	>90%	Outstanding (Very Low Risk)	Proceed
3–9	75%–90%	Good (Low Risk)	Proceed
1.5–3	60%–75%	Acceptable (Moderate Risk)	Proceed With Caution
0.8–1.5	44.4%–60%	Marginal (High Risk)	Delay or Corrective Action
<0.8	<44.4%	Unacceptable (Very High Risk)	Corrective Action or Shut Down

In addition, the decision maker may observe the predicted probability of success measurements or success factors at future Knowledge Checkpoints, especially the Full Operating Capability (FOC) Knowledge Checkpoint—the final milestone. A success factor greater than 1 at FOC, indicating that success is more likely than failure as the ultimate program outcome, would help to support the decision to proceed. A success factor less than 1, indicating that failure is more likely than success as the ultimate program outcome, would help support the decision for "Delay," "Corrective Action," or "Shutdown." Depending on the observations of evidence, the predicted probability of success at future Knowledge Checkpoints may indicate a different trend for success as compared to the assessment at the current Knowledge Checkpoint. It provides an additional insight into the program.

Case Analysis

A total of 14 case analyses were conducted as part of the DAPS research. Two of them were conducted with a prototype Bayesian network model based on the Naval Probability of Program Success v2 framework (Department of the Navy, 2012) for direct analysis and comparison. Twelve more case analyses were conducted on the final DAPS model. One of them is presented in the discussion that follows.

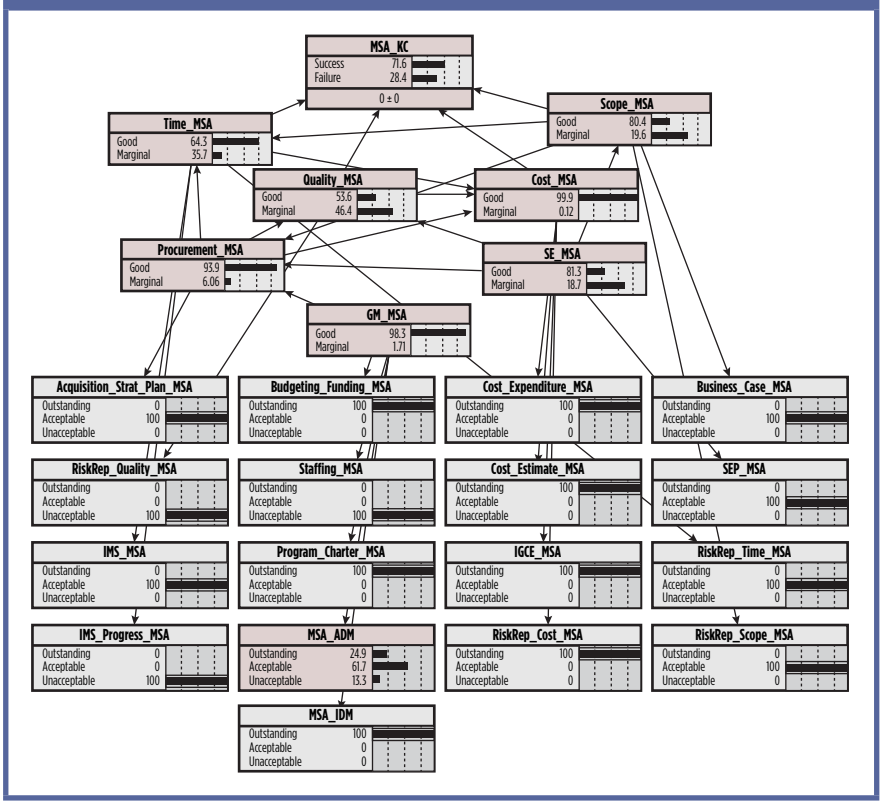
The intent of this case analysis is to test the sensitivity of the model to extreme but realistic conditions and analyze the effect of conflicting evidence on program success. The case presents a hypothetical program where program management, budgeting, and funding support are strong, along with an outstanding cost estimate, while contracting/procurement actions are proceeding with adequate performance. However, staffing is determined to be inadequate. The program also has not developed an SEP or any architecture. Quality risk is high due to the lack of technology maturity. This case is applied at Milestone A, and the DAPS model is being used to support the Milestone Decision Authority (MDA)'s milestone decision. The specific Evidence Node observations in DAPS appear in Table 4.

TABLE 4. SPECIFIC EVIDENCE NODE OBSERVATIONS IN DAPS

Acceptable Business Case	Pre-Engineering Development (PreED) Review
Unacceptable Risk Report (Scope) due to no architecture development to adequately define the program scope	Unacceptable manning/staffing
Unacceptable (missing) Systems Engineering Plan	Outstanding decisions outcome through the Investment Decision Memorandum (IDM)
Acceptable procurement progress and output—Acceptable acquisition strategy	Unacceptable Quality Risk Report due to technology maturity issues
Acceptable Integrated Master Schedule (IMS) and IMS progress and Acceptable schedule risk	Outstanding cost estimates
Outstanding program charter	Milestone Acquisition Decision Memorandum (ADM) is unobserved since decision has not been made

The model's Evidence Node observation inputs as well as the Knowledge Area Node and the Knowledge Checkpoint Node results are shown in Figure 5. The probability of success measure at this Knowledge Checkpoint, as indicated by the Milestone A Knowledge Checkpoint Node, is at 55.8%. This is the result of the model even with only four unfavorable observations as compared to 12 favorable. The program's time knowledge, cost knowledge, procurement knowledge, and general management knowledge are likely to be good; while scope knowledge, systems engineering knowledge, and quality knowledge are likely to be marginal.

FIGURE 5. CASE ANALYSIS OUTPUT AT MILESTONE A



The probability of success measurement at Milestone A is derived from the scope, quality, time, and cost Knowledge Area measurements. Although the evidence at this Knowledge Checkpoint strongly supports that the program has attained Good knowledge in the time Knowledge Area at 79.6%, and in the cost Knowledge Area at 99.9%, the evidence

does not support the same argument for the quality Knowledge Area and scope Knowledge Area, measured only at 41.4% Good and 37% Good, respectively. From the elicitation of the expert knowledge conducted in the research, the DAPS model specified the weighted influences of quality Knowledge Area and scope Knowledge Area to be twice as strong as the weighted inferential forces of time and cost Knowledge Area, producing the 55.8% Success measurement for Milestone A Knowledge Checkpoint.

Figure 5 outlines the probability of success for the case analysis at each of the 15 Knowledge Checkpoints and their respective success factors, based on the observation inputs at Milestone A.

Based on the success factor of 1.26 at Milestone A, the Knowledge Level of the acquisition program is rated as Marginal with a recommended action of Delay or Corrective Action. The fact that the future success factors past Milestone A are all above 1 bodes well for this program, however, indicating that the program contains a solid foundation for possible future success. Within the DAPS model, this can be attributed to the high general management Knowledge Area and cost Knowledge Area results. The general management Knowledge Area acts as the root node in each Knowledge Checkpoint instance computation, and has a strong influence on the other six Knowledge Areas. The cost Knowledge Area is the only leaf node within the Knowledge Area network structure and is a strong indicator of the adequacy of the other Knowledge Areas.

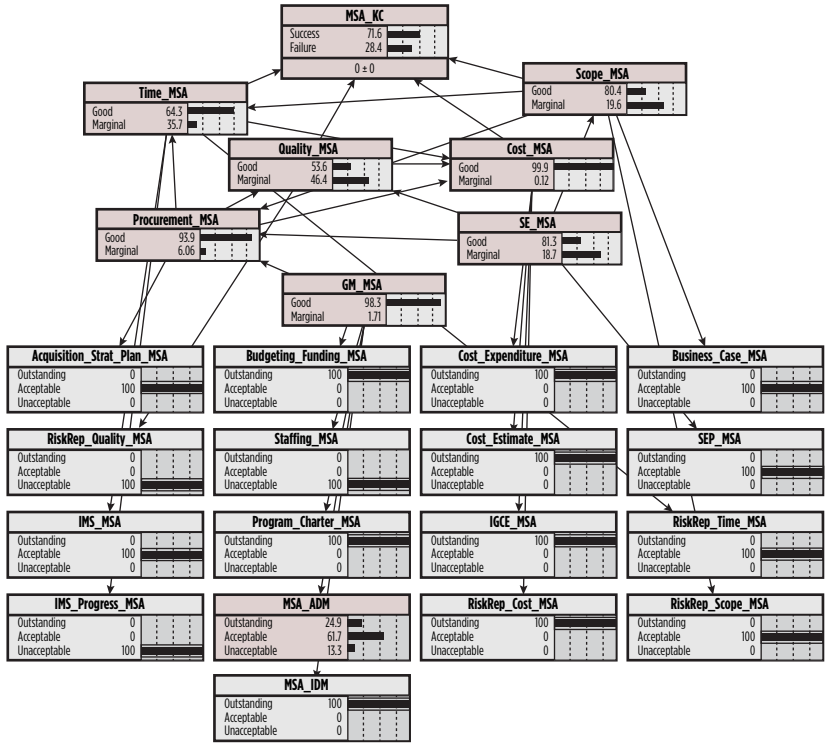
With the "Marginal" rating and recommendation of "Delay or Corrective Action," sufficient evidence is not present to either defend a favorable decision to proceed or unfavorable decision to shut down the program. However, the predicted future success factors indicate there are favorable observations of evidence supporting the likelihood for eventual success.

With the Marginal rating and recommendation of Delay or Corrective Action, available evidence is not sufficient either to firmly defend a favorable decision to proceed or unfavorable decision to shut down the program. However, the predicted future success factors indicate available observations of evidence support the likelihood for eventual success. Based on this DAPS assessment, the MDA would be advised to delay the Milestone A decision until the SEP and architecture artifacts are adequately developed. By that time, the program could be reassessed based on the developed artifacts and the program's approach to address the staffing shortage and technology maturity issues.

What-if Analysis

Prior to the actual Milestone A Review, the program manager might ask the question, "What if the Milestone A Review were delayed beyond the threshold date for a short period in order to develop the SEP and the architecture to an adequate level? What would that do to my probability of success measurement at Milestone A and beyond?" Figure 6 provides the Milestone A output from DAPS if the SEP and the scope risk level becomes acceptable, while the Integrated Master Schedule (IMS) Progress becomes Unacceptable due to the missed Milestone. This "what-if" scenario assumes all other observations of evidence for this case remain the same.

FIGURE 6. "WHAT IF" ANALYSIS AT MILESTONE A



Note. ADM = Acquisition Decision Memorandum; GM = General Management; IDM = Investment Decision Memorandum; IGCE = Independent Government Cost Estimate; IMS = Integrated Master Schedule; KC = Knowledge Checkpoint; MSA = Milestone A; RiskRep = Risk Report; SE = Systems Engineering; SEP = Systems Engineering Plan; Strat = Strategic.

As shown in Figure 6, if the program manager worked to complete the missing artifacts and delayed the Milestone A Review beyond the acceptable range, the probability of success at Milestone A would have been improved from 55.8% to 71.6%, which updates the success factor from 1.26 to 2.52, thereby doubling it. A success factor would have changed the Knowledge Level rating from Marginal to Acceptable and Recommended Decision from Delay or Corrective Action to "Proceed with Caution." The significant change can be attributed to two observations of evidence being changed to favorable, while only one is being changed from unfavorable to favorable: (1) the relative higher weight of scope Knowledge Area to Knowledge Checkpoint Success as compared to time Knowledge Area, and (2) the overarching effects of systems engineering Knowledge Area to the other Knowledge Areas.

Thus, if the program manager delayed the Milestone A Review until the SEP and the architecture were completed, the program manager would have provided the MDA better evidence to support a favorable decision to proceed, as compared to the original scenario. Even though falling behind schedule is undesirable, the what-if scenario with the Acceptable rating provided the MDA just enough proof of program maturity and knowledge certainty to be allowed to Proceed with Caution.

Conclusions

The DAPS model demonstrated the potential of an evidence-based, Bayesian network model to support acquisition decision making. DAPS quantitatively assesses a program's likelihood for success by building an inference network consisting of observable quality evidence, intermediate subject Knowledge Areas, defense acquisition Knowledge Checkpoints, and the respective CIRs among them. DAPS embodies the principles of knowledge-based acquisition in its ability to analyze DBS programs' knowledge and certainty levels through the Knowledge Checkpoint and Knowledge Area measurements. Through these quantitative measures, DAPS can be used to aid the acquisition decisions at Knowledge Checkpoints, whether to allow the program to proceed, delay, order corrective actions, or shut down the program.

The DAPS model represents an initial step toward modeling and analyzing the complex decision process for DBS acquisition and system development projects in general. Future research can be made to expand the Bayesian network presented within the DAPS model, further build

out the underlying complex interrelationships as well as environmental effects, and further develop the prescriptive capabilities to recommend decisions and actions. Potentially significant capabilities and enhancements could be achieved when coupled with the ever-advancing data science and computing power. Through the utilization of analytics to represent the information and evidence available and make better inferences the decision makers will be able to arrive at better informed decisions, leading to more successful programs and desirable investment outcomes.

References

Bloch, M., Blumberg, S., & Laartz, J. (2012, October). *Delivering large-scale IT projects on time, on budget, on value*. McKinsey & Company Insights and Publications. Retrieved from http://www.mckinsey.com/insights/business_technology/delivering_large-scale_it_projects_on_time_on_budget_and_on_value

Defense Acquisition University. (2013). *Defense acquisition guidebook*. Retrieved from https://dag.dau.mil/Pages/Default.aspx

Department of Defense. (2011). *Department of Defense source selection procedures*. Washington, DC: Office of Defense Procurement and Acquisition Policy.

Department of the Navy. (2012). *Naval PoPS guidebook—A program health assessment methodology for Navy and Marine Corps Acquisition Programs Version 2.2*. Washington, DC: Author.

Government Accountability Office. (2005). *NASA: Implementing a knowledge-based acquisition framework could lead to better investment decisions and project outcomes* (Report No. GAO-06-218). Washington, DC: Author.

Government Accountability Office. (2011). *Defense acquisitions: Assessments of selected weapon programs* (Report No. GAO-11-233SP). Washington, DC: Author.

Government Accountability Office. (2012). *DoD financial management* (Report No. GAO-12-565R). Washington, DC: Author.

Neapolitan, R. E. (2003). *Learning Bayesian networks*. Upper Saddle River, NJ: Prentice Hall.

Norsys Software Corp. (2010). *Netica 4.16 for MS Windows* [Computer software]. Vancouver, Canada: Norsys Software Corp.

Pearl, J. (1988). *Probabilistic reasoning in intelligent systems: Networks of plausible inference*. San Francisco, CA: Morgan Kaufmann.

Project Management Institute. (2008). *A guide to the project management body of knowledge (PMBOK guide)* (4th ed.). Newtown Square, PA: Author.

Schum, D. A. (2001). *The evidential foundations of probabilistic reasoning*. Evanston, IL: Northwestern University Press.

Author Biographies

Dr. Sean Tzeng is currently one of the lead enterprise architects at the Office of the Department of the Navy Chief Information Officer (DON CIO). He has previously supported Naval Sea Systems Command at several positions, performing systems engineering, architecture, and acquisition program management functions. Dr. Tzeng holds MS and PhD degrees in Aerospace Engineering and Systems Engineering/Operations Research from George Mason University.

(E-mail address: sean.tzeng@navy.mil)

Dr. K. C. Chang is currently a professor of systems engineering and operations research, and the director for the Sensor Fusion Lab, Systems Engineering and Operations Research Department, George Mason University. He holds MS and PhD degrees in Electrical Engineering from the University of Connecticut. Dr. Chang is an Institute of Electrical and Electronics Engineers Fellow, a position he earned for his contribution on sensor data fusion and Bayesian inference.

(E-mail address: kchang@gmu.edu)

Does Your CULTURE Encourage INNOVATION?

CDR Craig Whittinghill, USN, David Berkowitz, and Phillip Farrington

For many years military leaders have been calling for the U.S. Armed Forces to be more agile, adaptive, and innovative in order to defeat future and emerging threats. To assist the military in this endeavor, the University of Alabama in Huntsville explored Department of Defense (DoD) culture at the organizational level. Having the proper organizational culture can improve performance by empowering members to interact better with their environment, to communicate

Keywords: *organization, culture, military, innovation, organic*

and act rapidly, and, perhaps most importantly, to innovate. If organizational culture does not encourage innovation, however, organizations can improve innovativeness through culture manipulation. By implementing identified actions that influence cultural attributes, culture can be modified, and subsequently organizations can improve innovativeness, enabling them to meet new and complex challenges.

Image designed by Diane Fleischer

Calls from Senior Leadership

Over the past several years, senior military leaders and DoD civilians have been calling for more military innovation and adaptability. Retired Chairman of the Joint Chiefs of Staff Marine General Peter Pace called on the military to become more adaptive and agile by applying "our experience and expertise in an adaptive and creative manner, encouraging initiative, innovation, and efficiency in the execution of our responsibilities" (Pace, 2006, p. 2). Retired Navy Admiral Mike Mullen, also a former Chairman of the Joint Chiefs of Staff, stated that "new asymmetrical threats call for different kinds of warfighters … smarter, lighter, more agile … only by applying our own asymmetric advantages—our people, intellect, and technology—can we adequately defend the nation" (Mullen, 2008, p. 4).

During the *Defense Strategic Guidance* briefing held in the Pentagon on January 5, 2012, President Barack Obama, former Secretary of Defense Leon Panetta, and Chairman of the Joint Chiefs of Staff Army General Martin Dempsey introduced a new military strategy that shifts strategic focus to the Pacific and Asia. In his remarks, Panetta commented that the military's "great strength will be that it will be more agile, more flexible, ready to deploy quickly, innovative, and technologically advanced. That is the force of the future" (Panetta, 2012).

Furthering a culture of innovation within the DoD will contribute to the achievement of these transformational visions. Senior DoD leaders have endorsed and promulgated a culture of innovation dating back to at least 2001 when former President George W. Bush challenged officers during a speech at the U.S. Naval Academy to "risk failure, because in failure, 'we will learn and acquire the knowledge that will make successful innovation possible'" (Williams, 2009, p. 59). Since his speech, DoD's culture of innovation has improved, as evidenced by former Secretary of Defense Donald Rumsfeld's 2006 testimony to Congress during which he stated that the DoD's culture is "changing from one of risk avoidance to a climate that rewards achievement and innovation" (Fairbanks, 2006, p. 37).

How can the DoD continue this trend? The recent research has produced some very interesting results outlined in this article, on organizational culture, which may provide at least part of the answer.

Culture and Innovativeness

Webster's Ninth New Collegiate Dictionary defines culture as "the customary beliefs, social forms, and material traits of a racial, religious, or social group" (Culture, 1990, p. 314). The DoD's culture is influenced heavily by its famous hierarchical, mechanistic organizational structure. Organizational structure is described as a continuum. A mechanistic structure is on one extreme of the organizational system continuum. Typically mechanistic structures have a process where problems and tasks are strictly defined via instructions and orders issued by superiors who receive information as it flows up to them. Information follows a vertical path up and down the chain of command, enabling superiors to maintain their command hierarchy (Burns & Stalker, 1966). Mechanistic structures (and cultures) are characterized as controlled, formalized, and standardized (Reigle, 2003), and mechanistic organizations operate to meet orders from management to avoid mistakes or disturbances. A widely accepted premise in the research literature is that a mechanistic structure can inhibit innovativeness (Beyer & Trice, 1978; Damanpour, 1991; Tsai, Chuang, & Hsieh, 2009). Therefore, one can reasonably conclude that the DoD's mechanistic structure and culture would inhibit innovativeness.

On the other extreme of the organizational system continuum is an organic structure and culture (Burns & Stalker, 1966). Organic structures are believed to foster innovativeness (Prakash & Gupta, 2008; Robbins & Judge, 2009; Walker, 2007). These structures adapt to unstable conditions and change. They are characterized by individuals performing their tasks outside of a clearly defined hierarchy, considering their understanding of the workload of the organization while accomplishing their tasks. Control of information flow no longer rests with superiors (Burns & Stalker, 1966). An organic organization can operate flexibly and adapt quickly to a rapidly changing environment (Jones, 2004). Organic cultural values encourage creativity and innovation (Jones, 2004; Lamore, 2009), and innovative behavior (Hartmann, 2006).

Fortunately, for a mechanistic organization such as the DoD, some organic subordinate units are possible. In fact, a blend of these opposite structures can be advantageous to an organization. This concept is particularly true of organic structures operating within mechanistic structures. For example, units or departments may have their own organic structures, but the overall culture of the organization outside the unit or department may be influenced by its mechanistic, formalized chain of command. Organic structures and cultures that exist within a hierarchical organizational structure improve performance and enable development of innovations while taking advantage of quick organization-wide dissemination and implementation of those innovations (Gresov, 1984, 1989).

Culture and structure interact with each other, creating organizations that either innovate well, implement innovations well, or achieve both depending on the combination of culture and structure type (Gresov, 1984; Prakash & Gupta, 2008). This idea that organic and mechanistic

culture and structure can exist simultaneously, even symbiotically, within one organization is demonstrated daily by naval forces afloat. This concept has been implemented for decades in the Command by Negation construct in which local commanders have the freedom to conduct warfare in their specified area of responsibility until guidance from the chain of command above redirects their efforts. Command by Negation fosters initiative and innovation, particularly at the subordinate organizational level (LeGree, 2004).

Despite a decade's long use of Command by Negation, the research literature lacks empirical evidence that describes the relationship between an organization's structurally defined culture and its proclivity for innovation. This study adds to the literature and provides insight into how an organization can manipulate its culture to become more innovative. The rest of this article details our data collection, analysis, findings, and managerial insights.

Data Collection

This study focused on surveying a representative sample large enough to provide statistical rigor. The surveyed sample comes from a unique Navy community of organizations that share a common goal. Even though it was not one cohesive unit, unity of purpose provided the members of this community a common bond. This group of professionals consisted of roughly 1,100 individuals composed of scientists, engineers, operators, trainers, academics, and requirements officers.

The sample consisted of individuals who were active duty Navy personnel, government civilians, and contractors. Demographics are displayed in Table 1, and as can be seen, many similarities exist between the sample and the comparison demographics.

Upon inspection, the sample demographics more closely match Navy Officer Corps demographics than overall Navy demographics, especially regarding gender and the percentage of Caucasians. This Navy community is also representative of a group of professionals, especially scientists and engineers. This can be seen both ethnically and by age in Table 1. These results are expected since the sample is made up of professionals with significant experience, closely matching percentages and trends from U.S. college graduates and the college-educated U.S. science and engineering labor force.

TABLE 1. STUDY DEMOGRAPHIC DATA

Gender	Study Demographics	Comparison Demographics	U.S. Navy Total Active Duty Force Demographic Data (Jan-Mar 2010) (U.S. Navy, 2010)	U.S. Navy Officer Corps Demographic Data (Jan-Mar 2010) (U.S. Navy, 2010)		U.S. College Graduates (Kannankutty, 2005)	U.S. College Educated Science and Engineering Labor Force (National Science Board, 2010)
Males	84.9%		84.2%	84.8%		50.6%	74%
Females	15.1%		15.8%	15.2%		49.4%	26%
Ethnicity							
Native American	2.0%		4.55%	0.69%		0.4%	1.5%
African American	3.6%		18.4%	8.29%		6.1%	5%
Hispanic	5.6%		18%	6.1%		5.1%	3.5%
Subgroup Total	**11.2%**		**41%**	**15.1%**		**11.6%**	**10.0%**
Asian Indian	1.2%						
Asian (Far East)	5.2%						
Asian (Middle East)	1.6%						
Asian (Total)	8.0%		5.59%	3.99%		6.7%	
Pacific Islander	2.4%		1.04%	0.33%		0.3%	
Subgroup Total	**10.4%**		**6.63%**	**4.32%**		**7.0%**	**14%**
Caucasian	78.5%		62.6%	81.1%		81.4%	84%
Age (in years)					**Age (in years)**		
20–30	15.1%				<=29	6.5%	11%
31–40	20.7%				30–39	26%	27.5%
41–50	38.2%				40–49	27.6%	27%
51–60	16.3%				50–59	23.9%	21.5%
61+	9.6%				60+	16%	14.5%

Although the sample generally reflects of the active duty Navy, U.S. college graduates, and the college-educated U.S. science and labor force, it is not reflective of gender percentages in all three groups, notably in U.S. college graduates (over 49% are women) (Kannankutty, 2005). When viewed holistically in Table 1, however, the sample is reflective of the active duty Navy, U.S. college graduates, and the college-educated science and engineering labor force. The sample is most reflective, though, of the Navy Officer Corps and the college-educated U.S. science and engineering labor force (Kannankutty, 2005; National Science Board, 2010; U.S. Navy, 2010). Because of the composition of this sample, it can broadly be considered a typical cross-section of the professionals who constitute the DoD.

Measuring organizational culture can be accomplished through the use of surveys and questionnaires (Ashkanasy, Wilderom, & Peterson, 2000; Kraut et al., 1996). Using self-report surveys, in particular, offers respondents the opportunity to report their own perceptions of reality. Rentsch (1990) stated that behavior and attitudes are determined by perceptions of reality and not objective reality, so recording respondent perceptions instead of attempting to record reality is appropriate (Ashkanasy et al., 2000). Thus, it was determined that using self-report surveys was the preferred means of measuring organizational culture and innovative climate within the DoD. Therefore, to collect data, a 7-point Likert scale survey was administered in March and June 2010 to evaluate perceived organizational culture and innovative climate.

A quick note on culture and climate is prudent. Climate describes organizational expectations for behavior and outcomes. People respond to those expectations by shaping their behavior to achieve positive results like self-satisfaction and self-pride (Scott & Bruce, 1994). Both culture and climate are associated with behaviors (Denison, 1990), culture being the shared values and norms that shape behaviors, and climate representing organizational expectations that shape behavior. Denison (1996) concluded that culture and climate are a common phenomenon and that each describes organizational social context. Culture and climate research should be integrative and not mutually exclusive (Denison, 1996).

To conduct this research, a sample of 251 individuals was obtained by administering the Perceived Organizational Culture and Innovative Climate Assessment Tool (POCaICAT), a survey developed specifically for this research. A thorough review of the literature was conducted to

find instruments for use that measure organizational culture (along the organic and mechanistic continuum) and innovative climate. Twenty-four candidate survey instruments were identified. Eleven of these surveys measure organizational culture and 13 measure organizational innovative culture or climate (Whittinghill, 2011). The POCaICAT Revision A was developed by combining two valid and reliable Likert scale surveys. Surveys combined were the Organizational Culture Assessment (Reigle, 2003), which measures organizational culture, and the Climate for Innovation Measure (Scott & Bruce, 1994), which measures innovative climate.

Reliability

The researchers used Principal Component Factor Analysis to produce principal components, which were used to create a scale with items that reflected the construct being measured. The test of reliability used was Cronbach's alpha (Cronbach, 1951). Cronbach's alpha is regarded as the lower bound on reliability for a set of congeneric measures (Bollen, 1989). It assumes each of the items within the scale contributes equally to the underlying trait (Zeller & Carmines, 1980). The alphas are reported in Table 2.

TABLE 2. RELIABILITY DATA FOR POCaICAT REVISION A

Principal Component	Cronbach's Alpha
Support for Innovation	0.95
Workforce Autonomy	0.808
Collaboration	0.807
Managerial Trust/Workforce Enthusiasm	0.774
Resource Supply for Innovation	0.555

As indicated by the reliabilities, the measures are relatively homogeneous for the construct they purport to measure. Typically, reliabilities greater than 0.70 are considered adequate for measurement analysis (Nunnally, 1978). All but one measure in our analysis met this standard. Resource Supply for Innovation had a Cronbach alpha score of 0.555. This score, however, is sufficient. Cronbach's alpha values at or above 0.50 have been cited as acceptable for research (Caplan, Naidu, & Tripathi, 1984; Nunnally, 1967; Pedhazur & Schmelkin, 1991). The POCaICAT Revision A also demonstrated face, content, and construct validity (Whittinghill, 2011).

Sample Size

A sample size of 251 was found to be large enough to provide statistical significance to this study. The single-sample *t* test, Analysis of Variance (ANOVA), and linear regression were used throughout the research. First, for the single-sample *t* test, a sample size of 251 allowed a 5% alpha, 80% power, and 0.251 effect size level for the statistical analysis. An effect size of 0.251 is within the small (0.2) to medium effect (0.5) size range for the *t* test (Cohen, 2009). For ANOVA, seven of 11 organizations surveyed produced enough responses to average 34 per organization, resulting in statistical analysis conducted at the 5% alpha, 83% power, and medium effect (0.25) size level (Cohen, 2009). Finally, for linear regression a sample size of 251 produced an alpha of 5%, power of 80%, and effect size of 0.175 for statistical analysis. An effect size of 0.175 is within the small (0.10) to medium effect (0.3) size range for simple linear regression (Cohen, 2009).

Before proceeding, a brief discussion on the concept of effect size is offered. Cohen (2009, p. 9) indicates that an effect size is "the degree to which the phenomenon is present in the population" or "the degree to which the null hypothesis is false." Therefore, if the null hypothesis is true, then the effect size for the treatment is zero. So if a null hypothesis is false, it is false to some degree, or effect size (a nonzero value). The larger this value is, the larger the degree of manifestation of the phenomenon. Larger sample sizes are needed to detect a smaller effect. According to Cohen (2009, p. 25), a small effect size is applicable for new research areas because in new research areas where "the phenomena under study are typically not under good experimental or measurement control or both ... the influence of uncontrollable extraneous variables makes the size of the effect small relative to these." A medium effect size is defined as "one large enough to be visible to the naked eye. That is, in the course of normal experience, one would become aware of an average difference ... between members of professional and managerial occupational groups (Super, 1949, p. 98)" (Cohen 2009, p. 26). Although this research is being conducted in a relatively new research area, consistent dissemination of, and response to, a reliable and valid Likert-scale survey amongst professional and managerial groups led us to determine an effect size in the small to medium range was appropriate. A sample size of 251, therefore, was large enough to produce statistically significant results.

Analysis

The primary research question being addressed in this study was "Is there a relationship between the perceived organizational culture and innovative climate of this Navy community?" To answer this question, a hypothesis was formulated: that there is a linear relationship between the perceived organizational culture and the innovative climate of this Navy community. Linear regression was used to test the hypothesis. Before proceeding further, however, it is appropriate to note that with a sample size of 251, the central limit theorem (i.e., the sampling distribution approaches normality as sample size increases) applies, and a normal population distribution was assumed (Sheskin, 2004).

Parametric statistical analysis (i.e., single-sample t tests supported by the nonparametric Wilcoxon signed-ranks tests, ANOVA, and Tukey's honestly significant difference [HSD] tests) performed between organizations produced results that indicated a correlation exists between an organization's perceived organizational culture and its perceived innovative climate.

To validate these findings, simple linear regression analysis of the data was conducted. This portion of the research sought to determine whether a relationship exists between organizational culture and innovative climate within the surveyed Navy community. For one independent factor (degree of organic/mechanistic culture), an effect size of 0.1 (considered small for simple linear regression), an alpha value of 5%, and a power of 80% simple linear regression analysis requires 783 results for statistical rigor. However, this was not achievable for the surveyed Navy community, so a medium effect size (0.3 for simple linear regression) was deemed sufficient as previously rationalized. The medium effect size (0.3) was then used to determine a required sample size. According to Cohen, only 85 results are required, so the sample achieved provided a range of small to medium effect size (Cohen, 2009).

In this research, 7-point Likert-scale data were considered interval data and analyzed with parametric statistical tests vice ordinal data analyzed with nonparametric statistical tests. This approach was appropriate since the robustness of parametric tests and their use with ordinal data were supported in literature (Labovitz, 1967; Norman, 2010). Additionally, it was appropriate to consider data from the POCaICAT Revision A to be interval-level data since the data are in 7-point Likert-scale format (Boone & Boone, 2012); the POCaICAT Revision A is

both valid and reliable as shown through Principal Component Factor Analysis; and normality is assumed through the central limit theorem (Allen & Seaman, 2007). Additionally, nonparametric tests were used to validate the parametric tests in this research, further demonstrating that the results are robust.

Regression analysis was conducted to quantify the relationship between perceived organizational culture (i.e., the independent variable) and perceived innovative climate (i.e., the dependent variable or response).

Results produced substantial evidence that a statistically significant relationship existed between:

1. The degree to which an organization perceives itself to be organic; and
2. The degree to which it perceives itself to be innovative.

Table 3 shows that this regression analysis was significant because the regression analysis *p*-value (<0.5%) was less than the accepted level of significance (5%), indicating the null hypothesis—that the slope of the regression line is zero—can be rejected, and therefore conclude that a linear relationship exists between the predictor and response (Montgomery, Peck, & Vining, 2006). Also, the lack of fit *p*-value is greater than the accepted significance level of 5%, indicating that the null hypothesis (the model is linear) cannot be rejected (Montgomery et al., 2006).

TABLE 3. REGRESSION ANALYSIS RESULTS

Perceived Innovative Climate Score = 1.14 + 0.706 (Perceived Organizational Culture Score)

Regression *p*-value	Lack of Fit *p*-value	R^2	R^2 Adjusted
<0.005	.413	48.4%	48.2%

Further, the coefficient of determination values R^2 and R^2 Adjusted indicate that the model explains over 48% of the variance of the data, so over 48% of the variation of the dependent variable can be explained by the independent variable (Downing & Clark, 1997). This means that over 48% of the variation in perceived innovative climate can be explained by perceived organizational culture. Further interpreting this score was rather subjective, but the closer the score is to 100% the better. Explaining over 48% of the variance of the data, then, could be improved,

but an R^2 Adjusted value of 48.2% (from Table 3) is a sufficient score for this study. Devore (1995) stated that the square root of the coefficient of determination (or correlation coefficient R) indicates strong correlation between variables when this value is greater than or equal to 0.8 and less than or equal to 1; medium correlation when this value is greater than 0.5 and less than 0.8; and weak correlation when this value is less than or equal to 0.5. The square root of the coefficient of determination (R^2 Adjusted) for this regression model is 0.694, indicating a medium level of correlation (or degree of linear relationship) between variables. For initial research, this is acceptable. Further, the assumptions of normality of the residual data, homogeneity of variance, and independence of the data were evaluated and none was violated (Whittinghill, 2011).

> ***The data suggest that organizations can improve innovativeness through culture modification.***

The discovered relationship revealed that the more organic an organization perceived itself to be, the more it perceived itself to be innovative. Therefore, the data suggest that organizations can improve innovativeness through culture modification. However, to accomplish this, an organization must understand which attributes to develop in creating a more organic culture and subsequently a more innovative organization.

The literature review provided supporting evidence that the principal components previously identified were the attributes that can be modified to create a more organic culture and innovative climate. From the literature review, 27 attributes were found that contribute to innovativeness. This was a large number of attributes to study, and they needed to be reduced to a more manageable size. Initially, the 27 attributes were evaluated for adequacy and similarities, with 19 of the attributes deemed

appropriate for further study (Whittinghill, 2011). These 19 attributes share some commonalities, so like attributes were grouped together and placed in broader attribute categories (Whittinghill, 2011).

Whittinghill identified five attributes:

1. Support for Innovation. This is an organization's encouragement of creativity and willingness to change. It entails communicating the importance of creative, innovative thinking and recognizing innovators. Of all the attributes, this one, according to a review of the research literature, is most closely related to an organization's affinity for innovativeness (Ashkanasy et al., 2000; Scott & Bruce, 1994).

2. Resource Supply for Innovation. This is defined as having time, manpower, and funding available to pursue innovative endeavors.

3. Collaboration. This is defined as a high rate of interaction among organization members. It is encouraged by valuing all organization members' thoughts and ideas, and by having open door policies.

4. Workforce Autonomy. This is defined as having the flexibility to approach problems the way an organizational member sees fit based on available information, free from groupthink, and not overly impeded by regulations.

5. Managerial Trust/Workforce Enthusiasm. This is best described as a workforce motivated by their work and trusted to perform their work without being micromanaged. Note that Principal Component Factor Analysis revealed a correlated relationship between managerial trust and workforce enthusiasm, so these attributes were combined into one.

These five attributes contribute to an innovative climate (Ashkanasy et al., 2000; Burns & Stalker, 1966; Damanpour, 1991; Kenny & Reedy, 2006; LeGree, 2004; Ruiz-Moreno, Garcia-Morales, & Llorens-Montes, 2008; Prakash & Gupta, 2008; Robbins & Judge, 2009; Roxborough, 2000; Walker, 2007). Of these five, support for innovation best represents an

innovative climate because it most directly influences organizational expectations for innovative behavior. Expectations influencing behavior are fundamental to the definition of climate (Scott & Bruce, 1994).

The workforce autonomy, collaboration, and managerial trust/workforce enthusiasm attributes together determine where on the organic/mechanistic continuum an organization falls (Whittinghill, 2011). Also, per the literature (Damanpour, 1991; Prakash & Gupta, 2008; Robbins & Judge, 2009; Walker 2007), these attributes have a causal relationship with an innovative climate. The literature also states that the resource supply for innovation attribute has a causal relationship and contributes to an innovative climate (Robbins & Judge, 2009; Ruiz-Moreno et al., 2008).

Taken together, support for innovation and resource supply for innovation define an organization's affinity for innovativeness. The degree to which collaboration, workforce autonomy, and managerial trust/workforce enthusiasm are present (or not) determines whether an organic or a mechanistic culture is present, and subsequently how it influences an innovative climate.

Since support for innovation is most closely related to an innovative climate, the other attributes were theorized, supported by the previously cited research literature, to influence directly an organization's support for innovation. This theory was successfully tested utilizing a mathematical technique called structural equation modeling (Whittinghill, 2011).

Creating an Innovative Organization

Structural equation modeling, as depicted in Figure 1, was employed to estimate attribute influence and theorize attribute relationships (Bollen, 1989). It provided an effective technique for quantitative analysis, based on a premise that determines to what level an organization supports innovation, and subsequently an innovative climate. The premise is influenced by three primary factors:

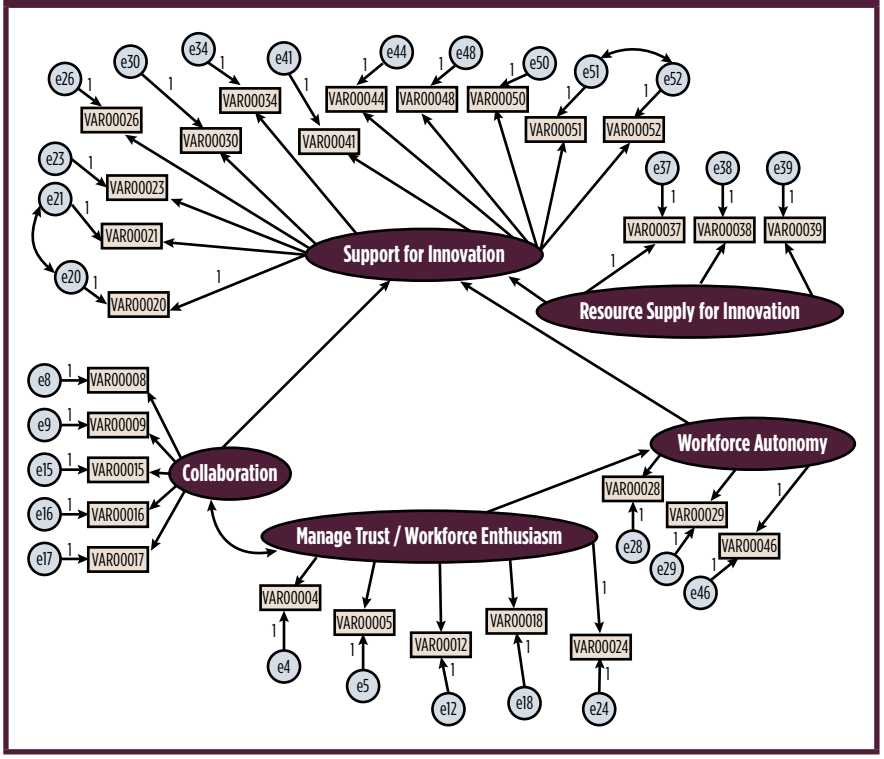
1. An organization's position on the organic/mechanistic continuum;

2. An organization's commitment to resourcing for innovation; and

3. Specific aspects of support for innovation represented only by manifest variables (made up of POCaICAT Revision A questions).

Additionally, structural equation modeling provided insight into the relationships between attributes that contribute to an innovative climate (i.e., the independent latent variables). The attributes modeled were the five attributes previously listed. The manifest variables (i.e., indicators) used were the questions of the POCaICAT Revision A (which were grouped according to the attributes they represent). Based on the causal relationships found in the literature review, a structural equation model was developed.

FIGURE 1. STRUCTURAL EQUATION MODEL FOR POCaICAT REVISION A



The derived structural equation model fit the data collected by the POCaICAT Revision A relatively well. This model produced an acceptable Root Mean Square Error of Approximation (RMSEA) value of 0.076

(Blunch, 2008; Byrne, 2010), an acceptable goodness of fit index of 0.797 (Kline, 2011), and an acceptable comparative fit index of 0.881 (Byrne, 2010; Kline, 2011), indicating a relatively good fit.

With model data fit established, the regression weights were reviewed (Table 4). All modeled relationships (displayed in Figure 1) between principal components were statistically significant and positive.

TABLE 4. STRUCTURAL EQUATION MODELING REGRESSION WEIGHTS

Latent Variable		Latent Variable	Regression Weight Estimate	Standard Error	Critical Ratio	*p*-value
Support for Innovation	←	Resource Supply for Innovation	1.87	.553	3.39	<.001
Support for Innovation	←	Collaboration	.688	.127	5.412	<.001
Support for Innovation	←	Workforce Autonomy	.266	.096	2.764	.006
Workforce Autonomy	←	Managerial Trust/ Workforce Enthusiasm	.798	.092	8.642	<.001

For the latent variables (i.e., attributes) resource supply for innovation, collaboration, and workforce autonomy, when the score of each on a 7-point Likert scale went up by one, the support for innovation latent variable would go up 1.87, 0.688, and 0.266, respectively. These regression weights (i.e., regression coefficients) predict the score of the support for innovation attributes (Arbuckle, 2007; Brewerton & Millward, 2006; Montgomery et al., 2006). If the managerial trust/workforce enthusiasm attribute went up by one, then the workforce autonomy latent variable would go up by 0.798 (and subsequently support for innovation would go up by 0.212). Thus, workforce autonomy has an indirect effect on the support for innovation attribute.

Conclusions

For this research study, a structural equation model was developed based on the results of a prior research literature review and populated with survey data from the DoD, which provided the basis for identifying the magnitude of attribute influence on innovativeness. The analysis of the model revealed that attributes influenced innovativeness to varying degrees.

1. Support for innovation has the greatest influence on innovativeness (per literature review and successful structural equation model using manifest variables).

2. Resource supply for innovation is the next most influential attribute (from structural equation modeling).

3. Collaboration is the third most influential (from structural equation modeling).

4. Workforce autonomy is a distant fourth (from structural equation modeling).

5. Managerial trust/workforce enthusiasm is the least influential, but almost as influential as workforce autonomy (from structural equation modeling).

Future efforts to further develop these attributes within an organization should consider each attribute's relative influence on innovativeness. Also, it should be understood that results may vary for different organizations and groups.

Before proceeding further, two quick notes are warranted:

1. Resource supply for innovation is extremely influential according to the structural equation model. Since personnel and funding allocated for innovative endeavors is expensive, providing time for such endeavors is the most practical resource to allocate.

2. As shown previously, collaboration, workforce autonomy, and managerial trust/workforce enthusiasm (if present in an organization) all have a positive influence on innovativeness, although to diminishing degrees.

Recently, DoD's senior leaders have promulgated several public statements promoting innovation throughout the DoD workforce. Linear regression analysis revealed that the more organic an organization perceived itself to be, the more it perceived itself to be innovative. This finding suggested that organizations can improve innovativeness through culture manipulation. If the culture does not encourage innovation, the most effective and practical actions to be taken to change the organizational culture and subsequently improve innovativeness, in priority order, are:

1. Communicate and demonstrate the importance of creative, innovative thinking.
2. Give members time to think innovatively.
3. Allow and encourage members to collaborate.
4. Allow members flexibility to approach problems as they see fit, free from group-think.
5. Assign motivating work and trust members to perform without being micromanaged.

By implementing these actions, culture within an organization can be modified to improve its innovativeness, to advance its ability to overcome future and emerging threats, and to meet new and complex challenges.

References

Allen, I. E., & Seaman, C. A. (2007). Likert scales and data analysis. *Quality Progress*. Retrieved from http://mail.asq.org/quality-progress/2007/07/statistics/likert-scales-and-data-analyses.html

Arbuckle, J. L. (2007). *Amos™ 16.0 user's guide.* Spring House, PA: Amos Development Corporation.

Ashkanasy, N. M., Wilderom, C. P., & Peterson, M. F. (Eds.). (2000). *Handbook of organizational culture and climate*. Thousand Oaks, CA: Sage.

Beyer, J. M., & Trice, H. M. (1978). I*mplementing change: Alcoholism policies in work organizations*. New York: Free Press.

Blunch, N. J. (2008). *Introduction to structural equation modelling using SPSS and Amos*. London: Sage.

Bollen, K. (1989). A new incremental fit index for general structural equation models. *Sociological Methods and Research*, 17(3), 303–316.

Boone, H., Jr., & Boone, D. (2012). Analyzing Likert data. *Journal of Extension*, 50(2). Retrieved from http://www.joe.org/joe/2012april/tt2.php

Brewerton, P., & Millward, L. (2006). *Organizational research methods*. London: Sage.

Burns, T., & Stalker, G. M. (1966). *The management of innovation* (2nd ed.). London: Tavistock.

Byrne, B. M. (2010). *Structural equation modeling with Amos* (2nd ed.). New York: Routledge/Taylor & Francis.

Caplan, R. D., Naidu, R. K., & Tripathi, R. C. (1984). Coping and defense: Constellations vs. components. *Journal of Health and Social Behavior*, 25, 303–320.

Cohen, J. (2009). *Statistical power analysis for the behavioral sciences*. New York: Psychology Press.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), 297–334.

Culture. (1990). *Webster's ninth new collegiate dictionary*. Springfield, MA: Merriam–Webster.

Damanpour, F. (1991). Organizational innovation: A meta-analysis of effects of determinants and moderators. *Academy of Management Journal*, 34(3), 555–590.

Denison, D. R. (1990). *Corporate culture and organizational effectiveness*. New York: John Wiley & Sons.

Denison, D. R. (1996). What is the difference between organizational culture and organizational climate? A native's point of view on a decade of paradigm wars. *Academy of Management Review*, 21, 619–654.

Devore, J. L. (1995). *Probability and statistics for engineering and the sciences* (4th ed.). Pacific Grove, CA: Duxbury Press.

Downing, D., & Clark, J. (1997). *Statistics the easy way* (3rd ed). Hauppauge, NY: Barron's Educational Series.

Fairbanks, W. P. (2006). Implementing the transformation vision. *Joint Forces Quarterly*, 42(3), 36–42.

Gresov, C. (1984). Designing organizations to innovate and implement: Using two dilemmas to create a solution. *Columbia Journal of World Business*, 19(4), 63–67.

Gresov, C. (1989). Exploring fit and misfit with multiple contingencies. *Administrative Science Quarterly*, 34(3), 431–453.

Hartmann, A. (2006). The role of organizational culture in motivating innovative behaviour in construction firms. *Construction Innovation*, 6(3), 159.

Jones, G. R. (2004). *Organizational theory, design, and change: Text and cases*. Upper Saddle River, NJ: Pearson/Prentice Hall.

Kannankutty, N. (2005). 2003 college graduates in the U.S. workforce: A profile. National Center for Science and Engineering Statistics InfoBrief (Report No. NSF 06–304). Retrieved from http://www.nsf.gov/statistics/infbrief/nsf06304/

Kenny, B., & Reedy, E. (2006). The impact of organisational culture factors on innovation levels in SMEs: An empirical investigation. *Irish Journal of Management*, 27(2), 119–143.

Kline, R. B. (2011). *Principles and practice of structural equation modeling* (3rd ed.). New York: Guilford Press.

Kraut, A. I., Ashworth, S. D., Bracken, D. W., Hinrichs, J. R., Johnson, R. H., Johnson, S. R., … Wiley, J. W. (1996). *Organizational surveys.* San Francisco: Jossey-Bass.

Labovitz, S. (1967). Some observations on measurement and statistics. *Social Forces*, 46(2), 151–160.

Lamore, P. R. (2009). *An empirical investigation of the antecedents of market orientation and organizational effectiveness* (Doctoral dissertation). University of Alabama in Huntsville.

LeGree, L. (2004). Will judgment be a casualty of network-centric warfare? *The Naval Institute: Proceedings*. Retrieved from http://www.military.com/NewContent/0,13190,NI_1004_NCW-P1,00.html

Montgomery, D. C., Peck, E. A., & Vining, G. G. (2006). *Introduction to linear regression analysis* (4th ed.). Hoboken, NJ: John Wiley.

Mullen, M. (2008). Priorities and strategic objectives of the Chairman of the Joint Chiefs of Staff. *Joint Forces Quarterly*, 48(1), 4–5.

National Science Board. (2010). *Science and engineering indicators 2010* (Report No. NSB 10–01). Arlington, VA: National Science Foundation.

Norman, G. (2010). Likert scales, levels of measurement and the "laws" of statistics. *Advances in Health Sciences Education*, 15(5), 625–632.

Nunnally, J. (1967). Psychometric theory. In E. J. Pedhazur (with L. P. Schmelkin), *Measurement, design, and analysis: An integrated approach* (1991). Mahwah, NJ: Lawrence Erlbaum Associates.

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

Pace, P. (2006). A word from the chairman. *Joint Forces Quarterly*, 40(1), 1–5.

Panetta, L. E. (2012, January 5). *Defense strategic guidance* [Pentagon press briefing]. Retrieved from http://www.defense.gov/home/features/travels/depsec.aspx

Pedhazur, E. J., & Schmelkin, L. P. (1991). *Measurement, design, and analysis: An integrated approach*. Mahwah, NJ: Lawrence Erlbaum Associates.

Prakash, Y., & Gupta, M. (2008). Exploring the relationship between organisation structure and perceived innovation in the manufacturing sector in India. *Singapore Management Review*, 30(1), 55–76.

Reigle, R. F. (2003). *Organizational culture assessment: Development of a descriptive test instrument* (Doctoral dissertation). University of Alabama in Huntsville.

Rentsch, J. R. (1990). Climate and culture: Interaction and qualitative differences in organizational meanings. *Journal of Applied Psychology*, 75(6), 668–681.

Robbins, S. P., & Judge, T. A. (2009). *Organizational behavior* (13th ed.). Upper Saddle River, NJ: Prentice Hall.

Roxborough, I. (2000). Organizational innovation: Lessons from military organizations. *Sociological Forum*, 15(2), 367–372.

Ruiz-Moreno, A. R., Garcia-Morales, V. J., & Llorens-Montes, F. J. (2008). The moderating effect of organizational slack on the relation between perceptions of support for innovation and organizational climate. *Personnel Review*, 37(5), 509–525.

Scott, S. G., & Bruce, R. A. (1994). Determinants of innovative behavior: A path model of individual innovation in the workplace. *Academy of Management Journal*, 37(3), 580–607.

Sheskin, D. J. (2004). *Handbook of parametric and nonparametric statistical procedures* (3rd ed.). New York: Chapman & Hall/CRC.

Super, D. E. (1949). *Appraising vocational fitness*. New York: Harper.

Tsai, M., Chuang, S., & Hsieh, W. (2009). Prioritization of organizational innovativeness measurement indicators using analytic hierarchy process. *The Business Review*, Cambridge, 12(1), 250–256.

U.S. Navy. (2010). *Navy-wide demographic data for second quarter FY 2010 (01 Jan 10 through 31 Mar 10)*. Millington, TN: Navy Personnel Command, Equal Employment Opportunity.

Walker, R. M. (2007). An empirical evaluation of innovation types and organizational and environmental characteristics: Towards a configuration framework. *Journal of Public Administration Research and Theory*, 18(4), 591–615.

Whittinghill, C. (2011). *An evaluation of the perceived organizational culture and innovative climate of a Department of Defense community of organizations* (Doctoral dissertation). University of Alabama in Huntsville.

Williams, T. M. (2009). Understanding innovation. *Military Review*, 89(4), 59–67.

Zeller, R. A., & Carmines, E. G. (1980). *Measurement in the social sciences*. Cambridge, UK: Cambridge University Press.

Author Biographies

CDR Craig Whittinghill, USN, is a career Naval Intelligence Officer, currently assigned as the Transnational Threats and Issues branch chief at U.S. Africa Command, J2-Molesworth. He is a graduate of the United States Naval Academy and the Naval Postgraduate School. CDR Whittinghill earned his PhD in Industrial Engineering with a concentration in Engineering Management from the University of Alabama in Huntsville.

(E-mail address: 95anchors@gmail.com)

Dr. David Berkowitz is dean of Graduate Studies and professor of Marketing at the University of Alabama in Huntsville. His current research focuses on the intersection between Product Development and Supply Chain for Complex Long Life Cycle products. His research has appeared in leading academic journals. Dr. Berkowitz earned his PhD in Marketing and Applied Statistics from the University of Alabama, an MBA from the University of Texas at Austin, and a BA in Accounting from Rutgers University at Camden.

(E-mail address: berkowd@uah.edu)

Dr. Phillip A. Farrington is a professor of Industrial and Systems Engineering and Engineering Management at the University of Alabama in Huntsville. He holds BS and MS degrees in Industrial Engineering from the University of Missouri-Columbia, and a PhD in Industrial Engineering and Management from Oklahoma State University. His research interests include systems engineering, transportation modeling, process analysis, innovation, and system performance measures.

(E-mail address: farrinp@uah.edu)

DoD Comprehensive Military Unmanned

AERIAL VEHICLE SMART DEVICE GROUND CONTROL STATION THREAT MODEL

Image designed by Diane Fleischer

Katrina Mansfield, Timothy Eveleigh, Thomas H. Holzer, and Shahryar Sarkani

In an effort to reduce costs and time to deploy mission capable unmanned aerial vehicles (UAV), the Department of Defense (DoD) has transitioned smart devices into the battlefield as portable, hand-held UAV ground control stations (GCS) without adequate cybersecurity protection. While a number of threat model approaches have been published, they are outdated and fail to evaluate a complete system. This article develops a holistic threat model that analyzes the cybersecurity vulnerabilities within the communication network, smart device hardware, software applications, as well as the insider threat. Additionally, this article provides a risk-based threat profile of a DoD pilot UAV smart device GCS system. This model will fill the gaps in current threat model approaches, to provide the DoD with a tool to properly assess the threat environment of a UAV smart device GCS, and build layers of security into the system throughout the system development life cycle.

Keywords: *acquisitions; process improvement; best practices; standardization; innovation*

With the rapid advancement of technology and its popularity in the consumer market, smart phones and tablets are migrating to and changing the way we operate on the battlefield. In the past, the Department of Defense (DoD) has been reluctant to allow smart devices to be used in a battlefield environment without the capability to provide secure connections for classified communication (Dalton, 2012). However, the enhanced capabilities and benefits of these small, handheld devices for mission planning and data sharing have persuaded the DoD to accept the inherent risks of using improperly secured smart devices on the battlefield. In fact, a number of these portable handheld UAV GCS devices are now part of a series of DoD pilot programs (Pellerin, 2013).

Background

UAV remote sensors often collect large amounts of data to be sent near real-time over a communication network for interpretation; however, current secured legacy military communication networks cannot support the large capacity needed to make this effective. Ultra High Frequency (UHF) satellite communication networks have been used to support UAV communication network requirements, but availability is limited only to the highest priority users and therefore is not always a viable solution (Wilcoxson, 2013). Other secured military wireless networks may be readily accessible, but share the same performance issues: processing capacity and latency limitations (Hartman, Beacken, Bishop, & Kelly, 2011). As a result, the DoD has explored solutions in the private sector to meet the rapidly evolving UAV communication requirements risking the use of unsecured networks.

Commercial smart phones and tablets provide the high processing capability needed to control and process data from UAVs in a compact, light-weight, mobile, handheld device. Using smart device technology and supporting software apps, the DoD has taken the functionality of a traditional GCS and miniaturized it into a mobile, portable smart device. These apps provide near real-time avionics flight display, navigation systems, system health monitoring and prognostics display, imagery and position mapping, and data processing (Troiani, 2011). Using a Fourth Generation (4G) Long Term Evolution (LTE) commercial wireless network solution provides a wide spectrum bandwidth, ranging from 1.4 to 20 megahertz (MHz); increasing the availability and options for operational frequencies for deployment. 4G LTE also significantly reduces

latency issues and provides peak data rate capabilities that feature near real-time data links with minimal interference from the UAV remote sensors (Hartman et al., 2011).

Several DoD pilot programs have been established to evaluate the technical capabilities of smart devices and demonstrate a proof of concept of the UAV smart device GCS. Previous research has explored cybersecurity threats to the UAV and the traditional GCS; however, little research has been done to explore what additional cyber threats have been encountered with the use of commercially available smart devices to command and control UAVs. Much of the technology and processes currently in development to secure the UAV smart device GCS system are not accompanied by a proper threat analysis. Current threat model tools are outdated and incapable of conducting a thorough threat analysis of an information system in its entirety, resulting in deploying inadequately secured devices to the battlefield, and increasing system and mission risk (Stango, Prasad, & Kyriazanos, 2009). Our research presents a recommended approach to conducting a threat model for information systems. By evaluating the vulnerabilities and threats to a DoD UAV within the parameters of a smart device GCS pilot program, both civilian and military UAV communities can benefit from the successful deployment of a properly secured UAV smart device GCS.

UAV Smart Device Case Study

Using a combination of Yin's Case Study Research approaches, the proposed threat model approach was developed to assess the security of the UAV smart device GCS (Yin, 2013). The first step involved a documentation review to assess the gaps in existing threat model approaches, followed by interviews to assess gaps in current government practices and the effectiveness of the proposed threat model. Lastly, direct observations of a pilot UAV smart device program were conducted to assess implementation of the proposed threat model.

Phase I: Threat Model Gap Analysis

The threat models currently being used are outdated and do not reflect advances in technology. Consequently, a number of gaps exist in the threat models being used to protect information systems. Threat models need to evolve with the technology and the associated threats (Stango et al., 2009). The gaps in the following sections address problems we found assessing a range of current threat models.

For the past 10 years, threat models have focused primarily on software applications. This focus is due in part to system failures and loss of data caused by software threats, including software viruses (Di & Smith, 2007). However, as technology has advanced in information systems, such as the UAV smart device GCS, threats are no longer limited to just software. Information systems today are comprised of hardware, software, and communication networks. Therefore, threats must be evaluated for the complete Unmanned Aerial System (UAS) within one single threat model to ensure the UAS is secured as a whole.

Little has been done in the development of threat models for hardware and communication networks, even though the number of attacks to hardware and communication networks has increased significantly with the advancement in technology and popularity of smart mobile devices (Wang, Streff, & Raman, 2012). Current hardware and communication threat models are tailored to specific systems or areas of interest. Recently, communication network threat models have been developed to address security concerns in personal networks; network jamming attacks; mobile ad hoc and sensor networks; and command, control, communications, computers and intelligence (C4I) security threats. Even fewer hardware threat models have been developed, only addressing hardware that has been compromised by malicious software logic and threats to storage systems. However, these areas of vulnerabilities have not been a major concern for the UAV community. Therefore, the need to improve upon these threat models has not existed.

With the exception of Clark et al. (2007), threat models have only addressed threats from malicious external attackers and not the internal threats and vulnerabilities that can arise from users or maintainers of the system. While system security is extremely important and must be maintained, the human factor is the biggest vulnerability in any system and is more critical than technology. Many of today's security problems are attributed to inadequate security awareness on the part of users

and maintainers, yet the majority of threat models do not address the internal human factors that can compromise system security (Chen, Shaw, & Yang, 2006).

A number of threat model methodologies exist; each has been tailored to fit the needs of a specific user and/or area of interest. A crucial, but often omitted step required within a threat model approach is a threat analysis. A threat analysis involves assessing the risk and prioritizing each threat and then determining the countermeasures to enhance system security. Threat models that fail to complete a threat analysis are incomplete, and do not provide designers with the information required to properly secure the system (Oladimeji, Supakkul, & Chung, 2006).

Threat Model Comparison. Table 1 introduces six published threat models and highlights critical gaps in the approaches that each describes. The following discussion further elaborates on these models and the gaps within each.

TABLE 1. THREAT MODEL COMPARISON

Threat Model Gaps	UAV Smart Device GCS Threat Model	A Hardware Threat Modeling Concept for Trustable Integrated Circuits	Threat Modeling for Mobile Ad Hoc and Sensor Networks	Security Threat Modeling and Analysis: A Goal Oriented Approach	Enhanced C41 Security Using Threat Modeling	Cyber Security Threat Analysis and Modeling of a UAV System
Identifies and addresses software threats	X			X		X
Identifies and addresses hardware threats	X	X			X	
Identifies and addresses network threats	X		X		X	X

Risk analysis and threat prioritization	X			X		X
Identifies and addresses human (inside/external) threats	X		X			

A Hardware Threat Modeling Concept for Trustable Integrated Circuits proposes a threat model approach to identifying hardware threats "to determine a circuit's trustability and provide guidance to malicious-logic checking tools" (Di & Smith, 2007, p. 1). This threat model is a simplified approach that involves understanding what the adversary wishes to accomplish and possible entry points, as well as identifying threats and attacks to the digital integrated circuits. While the need to determine the severity of threats and attacks as discussed, the threat model fails to identify a recommended approach rendering this threat model approach to hardware incomplete. While identifying threats is important to the security of device, this threat model approach doesn't provide information to make a determination on how to proceed forward with securing the device.

Threat Modelling for Mobile Ad Hoc Sensors Networks, as demonstrated by Clark et al. (2007), introduces a threat-model approach for mobile ad hoc networks and sensor networks. This threat-model approach characterizes the network system based upon military operation modes in peace-time, transition to war, and wartime; recognizing the variations of system context and operation may impact the risk decision making. Focusing on the adversary, this threat model attempts to identify what capabilities the adversary may have that may present a threat to the communication network. Based upon the operational environment and adversary capabilities threats to the network communications, infrastructure and services, physical nodes and people are identified. This threat model addresses a need for a risk-management approach to make a determination for what threats pose the greatest risk and an approach to addressing those threats. The threat model, however, fails to identify or even mention the need for countermeasures.

Oladimeji et al. (2006), in their Security Threat Modeling and Analysis: A Goal-Oriented Approach, uses a negative softgoal or N-softgoal approach to identify threats to software applications. This simplified threat-model approach defines security objectives for the system,

identifies software threats, analyzes threats and their associated risks, and provides a mitigation plan for countermeasures. This approach is effective for addressing software applications only.

Enhanced C4I Security Using Threat Modeling identifies a threat-modeling approach to C4I systems to protect sensitive military information being exchanged between information systems (Alghamdi, Hussain, & Faraz Kahn, 2010). The threat-model approach utilizes a variation of the negative softgoals approach described earlier in conjunction with the use of existing DoD architecture framework (DoDAF) artifacts. DoDAF operational view and system view diagrams are used to decompose and identify the operational needs of the system, interconnections, boundaries, scope, interfaces, entry and exit points, access points, attack points, and need lines. Using N-softgoal trees, threats and countermeasures to the system are identified based upon breaches to confidentiality, integrity, and availability security principles. The threat-model approach vaguely addresses the hardware threats, focusing primarily on the communication network. While the threat model identifies countermeasures for each system threat, the threat model fails to address a risk-analysis approach, thereby giving the impression that each mitigation technique or countermeasure should be implemented. Implementation of each countermeasure will not only drive up significant costs to the program but it may also impact the overall performance of the system.

Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System is intended to provide a threat model approach for a traditional UAV system; however, the threat-model approach focuses mainly on the communication link between the UAV and the traditional GCS (Javaid, Sun, Devabhaktuni, & Alam, 2012). The threat model identifies threat attacks to the confidentiality, integrity, and availability of the communication network, with mere acknowledgement of software threats to the UAV and GCS. A risk analysis is conducted of the communication network using flight simulation software; however, the approach fails to identify countermeasures and a mitigation plan. While the threat model discusses the components of the UAV system for background purposes, it is not considered part of the threat model and therefore may explain why the complete system is not assessed.

Threat modeling is a powerful tool that is critical to a system's security if used properly by the security team. Threat models provide the foundation on which threats will be identified, addressed, and mitigated. Table 1 identifies the gaps that exist within current threat models. Our proposed

threat-model approach is the first research-based model that addresses the UAV smart device GCS while also addressing existing gaps in threat models and government security practices. This robust threat model for the UAV smart device GCS will fill the gaps identified in current threat models and improve on existing techniques by addressing threats to all areas of an information system (hardware, software, communication network, and people), and conducting a thorough threat analysis by completing a risk assessment and providing countermeasures for the threats identified.

The threat model should be implemented throughout the system development life cycle and other government processes to enhance the security of the UAV smart device GCS. Identified threats that pose the greatest risk must be addressed in the UAS's security requirements, since those risks cannot be allowed to manifest if system security is to be ensured. This will help ensure security is built into the system, making both the government and defense contractors responsible for implementing the overall security of the device. The system design, accordingly, is influenced by the countermeasures implemented to mitigate threats to the system (Myagmar, Lee, & Yurcik, 2005). Security testing is conducted based on threat analysis to ensure that the final UAV smart device GCS system will be protected from the threats identified prior to deployment and to prevent attacks once the UAV smart device GCS system is fielded (Wang et al., 2012). Once the system is deployed, the threat model will need to be updated to reflect the changing threat environment and changes to the UAV GCS and the UAS. These are made to ensure that system security is maintained.

> ***Poorly written security requirements that fail to hold the program manager or the defense contractor accountable for implementation of specific security parameters will be outweighed by costs, resources, mission requirements, time constraints and politics to meet the program schedule.***

Phase II: Conduct Interviews

Security gaps in government systems. Cybersecurity has become a major focus for both the defense and commercial industries due to the growing number of publicized cybersecurity breaches to both industries. While the government is making strides to address cybersecurity in both the workplace and battlefield, we must first understand where the gaps exist. Thirty information assurance and cybersecurity subject matter experts in areas of policy, certification and accreditation, design, implementation, and test evaluation were interviewed to evaluate the existing gaps in the DoD processes for cybersecurity. This group exposed trends and showed existing gaps in policy, personnel, and threat models.

Security policies have been written vaguely and are often open for interpretation. Implementation of these policies has been at the discretion of the program managers who may not completely understand what is required, and therefore fail to dedicate the personnel and financial resources. Poorly written security requirements that fail to hold the program manager or the defense contractor accountable for implementation of specific security parameters will be outweighed by costs, resources, mission requirements, time constraints, and politics to meet the program schedule. Once the system reaches information assurance accreditation and certification, the system design is complete and ready for deployment. The cost to address the security of a deployment-ready system is significantly higher than at the start of the program. As a result, the program manager will most often be forced by schedule constraints to accept the security risks to meet the program schedule, budget constraints, and warfighter need.

Information assurance and cybersecurity expertise over the years has been synonymous with security policies, accreditation, and certification; however, programs need cybersecurity subject matter experts that are also knowledgeable about the system (hardware, software, and communication networks), systems engineering, and test and evaluation processes. Ideally, security teams with this expertise will help to ensure all components of the system have been properly secured and addressed throughout the entire system development life cycle. However, the resources and personnel to support each respective program are often limited or not available. Accountability for properly securing the system has been the sole responsibility of the government; the government must sufficiently address the security of the system in the requirements section of the contract to enforce shared responsibility

with defense contractors. This will help to build security into the system and fill the personnel gaps and expertise that currently exist within the government.

While threat models are being used by the DoD to evaluate cybersecurity vulnerabilities to military systems, no standard approach for threat modeling exists. Every program has a different perspective and definition of what a threat model is and how it is used. Threat models are often classified because of the type of data they collect (e.g., threats and vulnerabilities). As a result, threat models are frequently classified and not stored at operating locations and development sites, limiting their value to the program. This critical data, however, should be made available as a tool for both the program manager and the security team to address the cybersecurity vulnerabilities of the system and to build security into the system throughout the development life cycle.

Phase III: UAV Smart Device GCS Threat Model Pilot Program

While the use of UAV smart device GCS is intended to enhance the mission planning tools, environmental awareness, and operational capabilities of a multimillion-dollar UAV to support soldiers in the field, the security of the system must be evaluated and embedded into the system design for safe operation. Development and implementation of the robust threat model for the UAV smart device GCS is a key tool to ensure a secure and a safe operational environment.

The robust threat model for the UAV smart device GCS is a seven-step process that will: (1) characterize the system, (2) understand the adversary's objectives, (3) identify system assets and vulnerabilities, (4) identify threats and attacks, (5) conduct threat analysis and prioritization, (6) identify countermeasures, and (7) determine the mitigation plan. The following discussion will elaborate on each step of the threat model approach using a DoD UAV smart device GCS pilot program for illustration in an unclassified, generalized manner to avoid discussion of sensitive data.

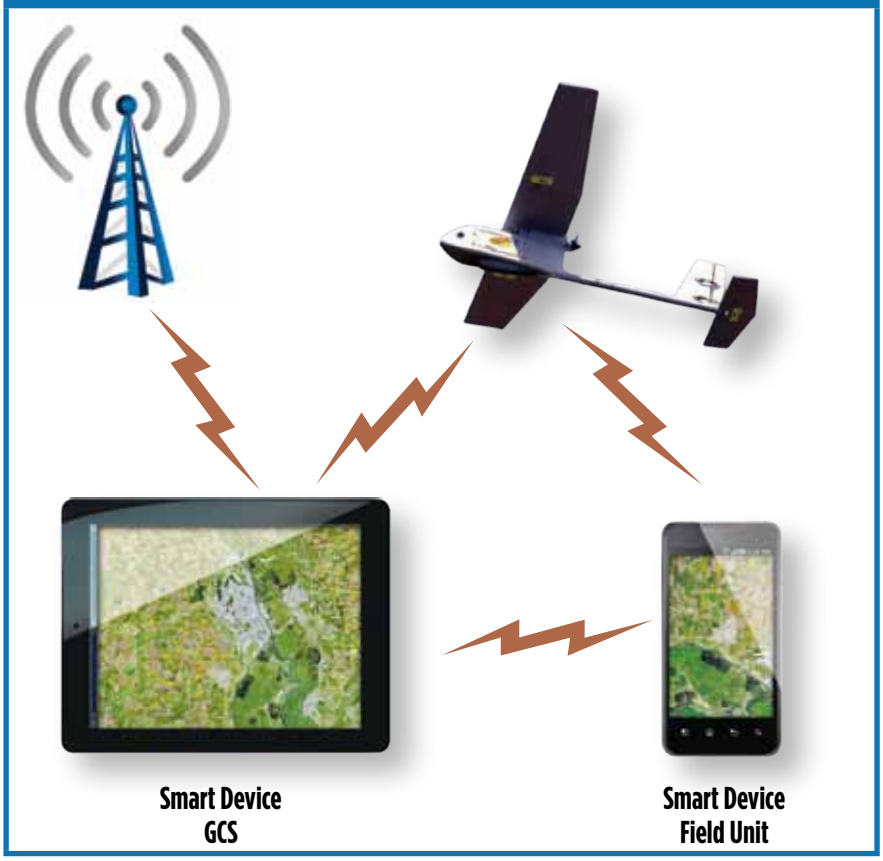
Step 1—Characterize the system. Characterizing the entire UAS is an important step in the threat modeling process, because it allows the security designer to understand the system and how it operates. While the overall goal of the threat model is to secure the UAV smart device GCS, the security countermeasures cannot hinder the functionality and the ability to meet mission capabilities and goals. Therefore, this

step establishes the intended functional operation for the system and identifies the relationship of components in the UAV smart device GCS system that meets mission goals (Torr, 2005). While the primary focus is to secure the UAV smart device GCS, the functional operation of the device is dependent upon other external components within the system such as the UAV, communication network, and other field units.

The TigerShark UAV is a mid-endurance tactical UAV with weapon capability used to support military intelligence, surveillance, reconnaissance, target identification, and weapons' deployment missions. The UAV smart device GCS system for the pilot program has four major components (Figure): the TigerShark UAV, the smart device Android tablet GCS, the smart device field unit, and the LTE 4G communication network. Depending on the type of mission, the UAV may be flown using a preprogrammed flight plan uploaded to the onboard computer or flown by a remote pilot who relies solely on the GCS to command and control the UAV (Mirkarimi & Pericak, 2003). The GCS software is installed on a 19-inch Android tablet and is used to command and control the UAV and its payloads, providing real-time avionics flight display, navigation, system health monitoring and prognostics display, graphical images and position mapping, and inward data processing. Conveniently, the smart device field units can receive intelligence data from the smart device GCS or directly from the UAV. Lastly, the pilot program will utilize 4G LTE communication network technology to provide the high performance, high bandwidth network for enhanced capabilities, and the data networking requirements needed to receive and share near real-time data with the UAV smart device GCS.

> ***While the use of UAV smart device GCS is intended to enhance the mission planning tools, environmental awareness, and operational capabilities of a multimillion-dollar UAV to support soldiers in the field, the security of the system must be evaluated and embedded into the system design for safe operation.***

FIGURE 1. UAV—SMART DEVICE GCS SYSTEM FUNCTIONAL DIAGRAM



Step 2—Understand the adversary's objectives. The previous step (Characterize the System) established the components and functionality of the system to identify ways the adversary will want to attack the system. It is important to note that the previous step identifies mission and functionality goals, while this step establishes the security parameters of the system, keeping in mind that the mission, functionality, and security goals are all intertwined, and all are equally important in the threat assessment of the system.

To properly defend the system, one must view the system the way an adversary would. To succeed in blocking the impacts of enemy attacks, the security team must first identify the adversary's objectives. The

key step here is to answer the question, what do the attackers want? (Myagmar et al., 2005). The output of this step will help to determine the vulnerabilities of the UAV smart device GCS in the next step.

The adversary's goal of attack on the smart device GCS is primarily to: (1) disrupt the operation of the device to prevent control of the TigerShark UAV, (2) gain control of the smart device GCS to control the TigerShark UAV, and (3) gain access to data that may be useful to the attacker. If the attacker is successful in any of these goals, the attacker can prevent completion of the mission (Yochim, 2010). These goals are often achieved through spoofing, tampering, repudiation, information disclosure, denial of service, and elevation-of-privilege attacks (Myagmar et al., 2005).

Step 3—Identify systems assets and their vulnerabilities. Using the information developed from the use case and adversary's objectives, this step identifies the assets and vulnerabilities specifically for the UAV smart device GCS system, which comprises the UAV smart device GCS and communication network only. An asset is an "abstract or concrete resource that a system must protect from misuse by an adversary" and is often an opportunity for attack (Myagmar et al., 2005, p. 3). Vulnerability is a security weakness or flaw that makes a system susceptible to attack (Oladimeji et al., 2006).

The UAV smart device GCS system is comprised of the hardware, software, and communication network components; therefore, we must assess these areas of vulnerability. Yet, we cannot properly assess the system without identifying vulnerabilities that are also introduced by the users and maintainers (Chirillo & Danielyan, 2005).

Hardware assets and vulnerabilities. The TigerShark UAV pilot program is utilizing an Android smart device tablet for the GCS. Hardware assets within the Android smart device tablet, such as the microphone, camera, and GPS, can be exploited to monitor the user and the users' surrounding environment (Delac, Silic, & Krolo, 2011). Memory storage can also contain classified information about the mission that can be useful to the attacker (Hasan, Myagmar, Lee, & Yurcik, 2005, pp. 94–102). Although the battery does not contain sensitive information, attackers can drain it to disrupt or terminate operation of the system (Delac et al., 2011). These threats can be introduced through malware software that enters through software and counterfeit hardware vulnerabilities.

Supply chain cybersecurity attacks have been a growing concern of the United States government since 2005, resulting in the seizure of large quantities of counterfeit network hardware and other information technology from Chinese telecommunication companies. Supply chain cybersecurity threats are introduced by hostile agents that purposefully install spyware into hardware components and/or alter circuitry with malicious firmware that is later sold to government and big businesses as counterfeit hardware (Goodwin, 2013). Once the electronic components are connected to the network, the enemy can easily gain access to it or, even worse, gain control of the electronic device to spy or cause harm. Unfortunately, many supply companies are transnational or the result of mergers, which makes it virtually impossible to adopt corporate ownership or control supply chain security of hardware components.

Another vulnerability is that enemies can gain physical access to the smart device GCS in a battlefield environment. A soldier under heavy fire can lose, drop, damage the device, or leave it behind in a life-and-death situation. The device can then be tampered with and analyzed to gain access to sensitive information stored in its memory.

Software assets and vulnerabilities. The heart of the smart device GCS is its mobile operating system, which controls its hardware resources and software applications. Infiltration of the operating system can be achieved through "jailbreaking," whereby restrictions and security measures can be removed to allow users to modify the device and install software applications. Once the attacker has found a way inside the system, it is easy to manipulate the hardware resources and transform the smart device into a device for spying that will allow the attacker to capture images and video, tap and record conversations, view sensitive information, and gain the location of targeted individuals (Felt, Finifter, Chin, Hanna, & Wagner, 2011, pp. 3–14). The pilot program is utilizing a smart tablet with an Android operating system. The software code has been made publicly available to allow customization and modifications to meet the needs of the various smart device types and communication carriers. The open operating system has resulted in many variations of Android smartphones and tablets whereby different carriers with identical devices may have different variations of the operating system software. Google security updates are pushed to the system's end users at the discretion of carrier and third-party application developers; depending on the complexity and time to make and test

> ***Software apps downloaded to the smart device are an easy target of cybersecurity attacks and must be protected by security mechanisms such as app certification or signature and pre-testing.***

modifications to tailor their devices, the carrier or third party software app developers may refuse to push the update to the end user, thereby increasing vulnerability to the smart devices (Rose, 2011).

Software apps provide the functionality of the GCS on smart devices. A successful attack on the software app could allow the attacker to gain control of the UAV functionality and access data gathered from the UAV, targeting individuals or locations for physical harm (Do, Kwon, & Moon, 2013).

Communication network vulnerabilities. In a tactical environment, ground soldiers are moving in a remote terrain where the coverage and performance of mobile networks are degraded and unsecure. Therefore, ground soldiers must provide their own secure, mobile networks to ensure continuous service (O'Rourke & Johnson, 2011). Stationary base stations establish a mobile network through a high-bandwidth, wired network backbone. However, if the ground soldiers move to another location, the mobile network is disrupted and inoperable until it is re-established.

Base stations are often attractive targets by hostiles desiring to disable the communication network. If the base station is destroyed, the secure communication network is inoperable, and ground soldiers will create their own insecure mobile networks or use insecure commercial networks. These actions introduce threats into the communication network, the devices operating on the network, and the missions they support (Bhargava, 2013). Direct attacks on the communication network can disrupt the connection between the UAV and the smart device GCS, thereby preventing operation and control of the UAV. They prevent the

sharing of information within the UAV smart device GCS system; and potentially share information with other unauthorized users (Clark et al., 2007).

Human vulnerabilities. Threat models often focus on external attackers and threats that can affect the system. What tends to be overlooked, however, is how users and maintainers of the system also pose a danger to the system. Users can accidentally or intentionally share sensitive information or physically compromise the system by disregarding policies and operating procedures, or fail to update policies and procedures aimed at current threats (Clark et al., 2007). Although smart devices have been deployed in the battlefield to function as UAV GCSs, they can also be used for many other capabilities that may be of interest to the unwitting user and introduce threats to the GCS. For instance, users and operators could access social networks and e-mail outside of battlefield operations, thereby increasing the chances that phishing, spam, malware, and spyware will infiltrate the system (Leavitt, 2011).

Maintainers of the smart device GCS play a crucial role in its security and also determine the effectiveness of countermeasures implemented within the device. Poorly maintained systems expose entry points of attack to gain control of the UAV GCS (Whitman & Mattord, 2010).

Step 4—Identify threats and attacks. Using the information gathered in the previous step, the next step is to identify threats and attacks to the system. As previously mentioned, a threat is defined as a "potential violation of the security of a system, an event that may have some negative impact," and an attack is an "exploitation of a vulnerability to realize a threat" (Oladimeji et al., 2006, p. 1). The threat identification process described in the following discussion examines threats in detail for four areas of vulnerabilities.

Hardware threats. Threats to the Android smart device GCS hardware include attacks that cause battery exhaustion, flooding, surveillance, and USB and storage attacks. Battery exhaustion attacks cause the battery to discharge faster than normal, killing the smart device and ultimately disabling the GCS. This prevents the operation and control of the UAV. Flooding attacks disable the smart device by overloading it with numerous signals or messages, preventing GCS operation or preventing it from providing or receiving information within the network (Bhusari & Sahu, 2013). Surveillance attacks employ smart device sensors to monitor the surrounding environment and soldier movement, which allows the

attacker to gain unauthorized access to mission information and identify the location of the soldier maneuvering the UAV and other soldiers nearby. Storage snooping attacks, a result of malware, allow the attacker to gain access to sensitive information via storage snooping attacks. Storage jamming and alteration attacks modify data for the purpose of subverting, degrading, or disrupting operations (Hasan et al., 2005).

Software threats. Mobile platforms resemble traditional desktop operating systems; therefore, the security threat profile of a personal computer has migrated to smart devices (Delac et al., 2011). Malware attacks gain access to a device to steal data, damage the device, or annoy the user. This threat includes Trojan horses, botnets, worms, key loggers, and rootkits (Felt et al., 2011). In addition, malware can be used to disrupt and gather sensitive information or obtain control of the GCS and UAV. Spyware collects personal information such as location and stored information (Felt et al., 2011). It can also be used to gather intelligence from UAV real-time data feeds or directly from the smart device GCS using the microphone, camera, GPS, or stored data to obtain mission-sensitive information. Data accessed by malware and spyware attacks can introduce data leakage and unauthorized data transmission. Malicious software also can be used to tamper with data by either destruction or modification (Bhusari & Sahu, 2013). Sensitive information or dangerous capabilities are often protected by requiring user consent before an application can gain access. However, elevation of privilege is a common attack achieved through software manipulation to gain access to resources that would otherwise be protected (Olzak, 2006).

Communication network threats. Threats to the communication network include network eavesdropping, spoofing, denial of service, impaired quality of service, jamming, weak/compromised cryptography, and unencrypted communication. Network eavesdropping or sniffing captures and decodes packets as transmitted over the network. Spoofing attacks masquerade the hacker as a trusted party in the network to gain access to sensitive information, which can lead to data leakage—the unauthorized transmission of sensitive data. Denial of service or network congestion overloads a link or node in the UAV smart device GCS system with an extensive amount of data to reduce the quality of network performance or cause denial of service (Spiewak, Engel, & Fusenig, 2006, pp. 35-40). Impaired quality of services, another form of denial of service, is an attack that degrades the level of performance or causes disruption of the network to prevent services required for applications, users, or data flow (Clark et al., 2007). Denial of service attacks not only threaten

the communication network, but also the UAV. False commands or control signals transmitted over the network to the UAV can make the UAV land or attack somewhere else (Javaid et al., 2012). A jamming device can disrupt and disable communication between the smart device GCS and UAV, and other components in the network, thereby preventing control of the UAV and dissemination of information within the network hub. Weak cryptographic algorithms are easily broken by attackers exposing sensitive data to adversaries. If the attacker intercepts the encryption key, the cryptography becomes compromised, and the network is exposed to data leakage. Sharing sensitive information using unencrypted communications allows for harmful data leakage to unauthorized parties (Clark et al., 2007).

Human threats. Threats to the UAV smart device GCS can also be introduced by system users and maintainers. In some instances, threats will enter the system due to careless mistakes or inadequate practices, such as the failure to follow policies or inadequate policies, use of unencrypted communication, carelessness with cryptographic keys, poor risk decisions, and poor management or maintenance. These threats can lead to data leakage, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protect information (Whitman & Mattord, 2010). Poor risk decisions can be the result of carelessness or a combination of poor training and the stress and limitations of completing missions in a battlefield environment. Insufficient management and maintenance of the GCS can compromise system integrity, hinder GCS performance, and even render it inoperable (Clark et al., 2007).

Compromised personnel acting as inside agents are another vulnerability. They can introduce threats such as harmful data leakage and could modify stored accountability information. Obvious threats from an inside agent include directing the GCS and UAV to conduct surveillance on and attack military personnel. Access to the GCS could also provide sensitive data to adversaries and lead to the destruction of sensitive data. Accountability information is extremely important in military applications, as users and maintainers are responsible for operating and maintaining a device that controls multimillion-dollar unmanned aircraft with weapon capabilities. In the event that an error occurs, poor decisions are made, or the device is compromised, accountability logs can be reviewed post-operation to connect actions to people. Accountability logs can be attacked by preventing the collection or storage of accountability information. By the same token,

deletion and modification of accountability information to shift blame or render it impossible to determine blame also has a negative effect on security (Clark et al., 2007).

Step 5—Conduct threat analysis and prioritization. The previous steps help to identify threats to UAV smart device GCSs. The next step analyzes threats by completing a thorough risk assessment of each threat to prioritize the threats and address countermeasures for high-risk attacks (Myagmar et al., 2005).

While it is impossible to guarantee 100 percent security of a system, it is important to identify the threats, prioritize their associated risks, and identify those that are most crucial for the UAV smart device GCS operational environment (Oladimeji et al., 2006). To assess the risk of identified threat attacks, the likelihood and impact are calculated using the National Institute of Standards and Technology (NIST) Management Guide for Information Technology Systems methodology (Stoneburner, G., Goguen, A., & Feringa, A., 2002). NIST is the designated authority for the development of information security standards and guidelines for federal government agencies and private industry. Since the UAV smart device GCS operational environment is being evaluated for military purposes, the NIST methodology is appropriate for assessing the risk and applied as follows.

Likelihood determination. The likelihood is the probability that a potential vulnerability will occur in the associated threat environment and considers threat-source motivation and capability, nature of the vulnerability, and the existence and effectiveness of current countermeasures (Stoneburner, Goguen, & Feringa, 2002). The following NIST criteria are used to rate the likelihood of the threats identified (Table 2).

TABLE 2. LIKELIHOOD DEFINITIONS

Likelihood Level	Likelihood Definition
High (1.0)	The threat source is highly motivated and sufficiently capable; controls meant to prevent the vulnerability from being exercised are ineffective.
Medium (0.5)	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low (0.1)	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Impact assessment. The impact assessment determines the level of impact to system assets and sensitive data based on protections required to maintain security goals (Stoneburner, Goguen, & Feringa, 2002). The following criteria are used to rate the impact of the threats to the handheld, portable GCS (Table 3).

TABLE 3. IMPACT DEFINITION

Magnitude of Impact	Impact Definition
High (100)	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium (50)	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low (10)	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Threat risk assessment results. Using the likelihood and impact criteria, analyzed threats to the UAV smart device GCS system (Table 4) with a team of cybersecurity and system subject matter experts. Likelihood was assessed using existing threat data. Current research, experience, vulnerabilities, and the ability of existing controls to minimize vulnerabilities to the TigerShark UAV smart device GCS were included in the evaluation. Impact was assessed based on effect on mission goals and objectives, physical damage to assets and resources (UAV, GCS, etc.), and potential death or injury to humans. The risk for each threat was calculated as the product of the impact and likelihood, and risks were assessed at the following NIST defined levels: High Risk (product value >50 to 100), Medium Risk (product value>10 to 50), and Low Risk (1 to 10) (Stoneburner, Goguen, & Feringa, 2002).

TABLE 4. RISK ANALYSIS SUMMARY			
Threat	**Likelihood**	**Impact**	**Risk**
HARDWARE			
Battery Exhaustion	0.5	100	50
Flooding	1.0	50	50
Surveillance	1.0	100	100
USB	0.1	10	1
Storage Snooping	0.5	50	25
Storage Jamming	0.5	10	5
Storage Erasure/Alteration	0.1	50	5
SOFTWARE			
Malware	1.0	100	100
Phishing	0.5	50	25
Data Leakage	1.0	50	50
Spyware	1.0	100	100
Data Tampering	1.0	50	50
Elevation of Privilege	1.0	100	100
COMMUNICATION NETWORK			
Eavesdropping	1.0	100	100
Spoofing	0.5	100	50
Denial of Service	1.0	100	100
Jamming	1.0	10	10
Weak/Compromised Cryptography	0.5	50	25
Unencrypted Communication	0.1	50	5
Impaired Quality of Service	0.5	100	100
HUMAN			
Breaking Policy	1.0	100	100
Inadequate Policy	1.0	100	100
Unencrypted Communication	0.5	50	25
Carelessness with Cryptographic Keys	1.0	50	50
Harmful Data Leakage	0.5	50	25
Compromise of Personnel	0.5	100	50
Poor Risk Decisions	0.5	100	50
Poor Management/Maintenance	1.0	100	100
Overloading the Operator	0.5	10	5
Prevention of Accountability from Being Stored	0.1	10	1
Destruction of Accountability Data	0.1	10	1
Modification of Accountability Data	0.1	10	1

Based on the above criteria, the risk assessment in Table 4 shows that surveillance attacks to the hardware, malware, and spyware attacks to the software; eavesdropping, denial of service, and impaired quality of service attacks to the communication network; and neglected or inadequate policy and poor management and maintenance practices pose the greatest risk to the UAV smart device GCS system. Of all these, malware is the most significant threat, because its likelihood is extremely high. The communication network is an important component to the UAS operation. As previously mentioned, the UAV smart device GCS pilot is utilizing 4G LTE network technology, a commercial communication network. While use of the 4G LTE network provides the communication network requirements for UAS operation in the battlefield, it doesn't provide the security of legacy military systems, thus increasing the risk of eavesdropping, denial of service, and impaired quality of service attacks. While there are solutions to secure the network during operation, performance degradation of the smart device GCS is an issue. Neglected or inadequate policies are a major vulnerability for UAV smart device GCSs. Neglected or inadequate policy can place the operator and other friendly forces on the battlefield in danger and compromise the security of the GCS and UAV. Poor management or maintenance of the UAV smart device GCS can weaken countermeasures embedded in the system and increase the risk of new threats to the UAS. These significant risks to the system should be given high priority and addressed with countermeasures.

Medium-high risk threats that require countermeasures include battery exhaustion and flooding attacks to hardware; data leakage and surveillance attacks to software; data tampering, and spoofing attacks to the communications network; and compromised personnel, poor management, and poor risk decisions. The military must evaluate the remaining threats, which include those of medium and low risk, and determine whether to implement countermeasures, based on performance and cost factors, or accept the risk.

Step 6 – Identify Countermeasures. Countermeasures are "techniques to protect the system" (Alghamdi et al., 2010, p. 3). This step identifies countermeasures to counteract the medium- and high-risk attacks to the UAV smart device GCS identified in the last step. While a number of countermeasures will be identified to reduce risk to the system, all countermeasures cannot be implemented due to costs and performance

degradation. Outputs from the threat analysis in the previous step will help to determine the combination of countermeasures for optimal protection with performance and costs.

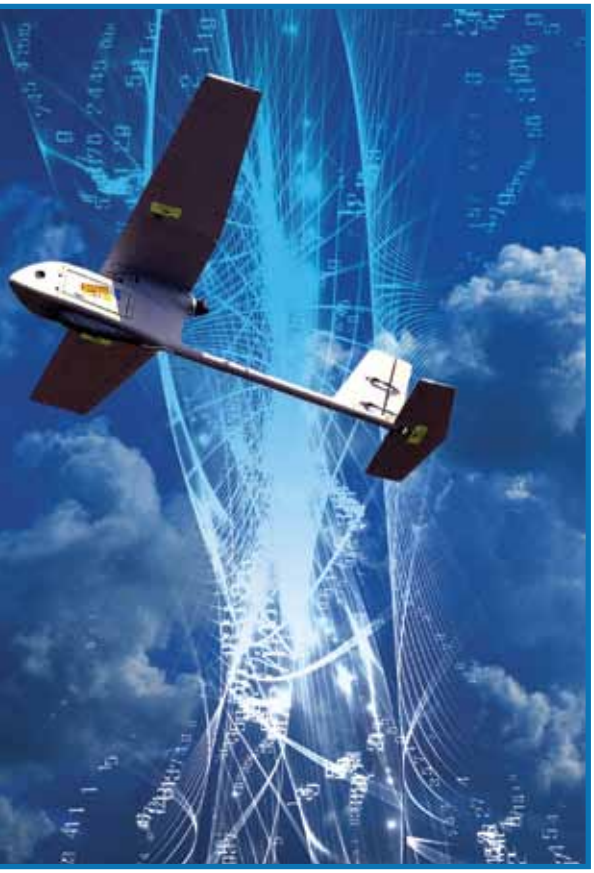
Hardware countermeasures. U.S. companies and agencies can reduce risk to counterfeit networking hardware by limiting purchases to trusted vendors. Companies can also conduct random tests on devices during the distribution and installation phases to determine whether they contain extra components or serious vulnerabilities (Lee & Rotoloni, 2012).

A Smart device GCS obtained by the adversary can be counteracted with security mechanisms such as authentication, encryption, and remote wipe. These techniques can protect against unauthorized access to classified or sensitive information. Authentication limits access and privileges to only authorized parties, detecting and preventing access by others. This can also be achieved with passwords and screen lock codes; however, they can hinder the quick response and performance of soldiers using the devices on the battlefield. Encryption encodes data to prevent disclosure of sensitive or classified data to unauthorized parties. It can also protect data at rest (i.e., files, memory, USB flash drives, etc.) when physical security fails (Wang et al., 2012). Meanwhile, remote wipe allows the smart device GCS to be commanded remotely. Therefore, it can be reset or, if the device falls into an unauthorized user's possession, stored data can be erased. This security mechanism can be evaded, however, by removing the battery or memory card prior to receiving the remote wipe command (Hasan et al., 2005).

Software countermeasures. Malware and spyware are the most common attacks to operating system software and software applications, and can have major consequences if not detected immediately. Frequent testing for malware can be done using fuzz testing and static-analysis code scanning test tools. Fuzz testing sends structured, invalid inputs to software application programs and network interfaces to detect errors that can lead to software vulnerabilities. Static-analysis code scanning test tools can detect specific kinds of coding flaws and software vulnerabilities (Lipner, 2004). The smart device GCS can also be protected using antivirus and firewall software. Antivirus software can prevent, detect, and remove malware from software applications and operating system software, whereas a firewall can prevent unauthorized access to and from the smart device GCS and access to unauthorized, untrusted wireless networks. Software applications often access hardware resources within the smart device beyond what is required for operation of the

app, increasing vulnerability of the smart device GCS. Access control limits accessibility to resources and/or services, only allowing the app to tap into the minimum resources needed (Jeon, Kim, Lee, & Won, 2011). Resource management monitors the availability and condition of resources (Shabtai et al., 2010).

Although smart devices will be used primarily as UAV GCSs, soldiers may be tempted to access personal e-mail and social networks, thereby introducing threats such as spam and phishing. Communication from outside the secure network should be blocked. Spam filters can also be used to prevent receipt of spam from unwanted parties via multimedia message service, text messages, e-mail, and telephone (Jeon et al., 2011).



Software apps downloaded to the smart device are an easy target of cybersecurity attacks and must be protected by security mechanisms such as app certification or signature and pre-testing. Application signatures should be used to ensure that the software is from a trusted source and has not been tampered with. Pretesting software apps by detecting malicious malware prior to use in the battlefield ensures that only secure apps will be uploaded to the software app database (Jeon et al., 2011).

Vulnerabilities to the software can be mitigated by regularly updating the operating system and software applications immediately after updates are released (Jeon et al., 2011).

Communication network countermeasures. Many threats to UAV smart device GCSs arise from deficiencies in network security. Flooding, jamming, denial of service, and impaired quality of service attacks can be mitigated by bandwidth allocation, which limits bandwidth for the smart device to prevent excessive connection request attacks that may impair network and affect the operation of the smart device

GCS. Eavesdropping and data leakage can be prevented by network encryption, which encodes data to prevent disclosure of sensitive data to unauthorized parties and can protect data in transit over shared networks. However, encryption policies and procedures must be updated periodically to ensure an adequate level of cryptography. Data transferred over the network can be protected by safe http data-transfer protocols, authentication certificates, data encryption and decryption, and virtual private networks (Markelj & Bernik, 2012). UAV GCS software requires consistent network access, but other software apps that support military operations may not (Clark et al., 2007).

In the past, network security concerns have hindered widespread smart phone deployment on the battlefield, but since 2010, the DoD has moved to enhance communication networks to accommodate the requirements for smart devices and UAV capabilities on the battlefield (Edwards, 2012). Stationary base stations, as previously discussed, didn't provide the infrastructure required for smart devices and UAVs, and therefore were inadequate for the current technology and enhanced capabilities (O'Rourke & Johnson, 2011). New technology advancements, such as mesh networks, mobile ad hoc networks, cognitive radios, and satellite communications have offered better options for mobile network availability on the battlefield. Mesh networks or mobile ad hoc networks provide high bandwidth networking capabilities to connect multiple smart devices within a specified range, control UAVs, and disseminate data feeds within the communication network. Cognitive radios can adapt to user needs and bandwidth conditions, providing quality system performance in all types of terrain. They are also resistant to eavesdroppers and jammers (Edwards, 2012). Advances in technologies such as antenna design and signal reception have made satellite communication networks a viable solution for smart devices on the battlefield. Satellite communication is ideal for coverage of terrestrial areas (Varshney & Vetter, 2000).

The effectiveness of countermeasures previously identified depends on the actions taken by users and maintainers to secure the system. Security countermeasures for the GCS can be significantly enhanced through security policies, education, training, and awareness (Chen, Shaw, & Yang, 2006). To reduce the risk of data leakage, policies and operating procedures should be updated periodically to reflect current mission requirements and threats. Security policy is important, as it defines the rules, guidelines, and procedures for proper use and protection of the system (D'Arcy, Hovav, & Galletta, 2009). In addition to updating

policy, users and maintainers must be made aware of all changes in policies and procedures, and be educated and trained periodically to stay abreast of the most up-to-date information. This will also make users and maintainers accountable for their actions on the battlefield. Security education, training, and awareness provide users and maintainers with information regarding the security environment and the skills required to perform security procedures and reinforce security policy awareness and comprehension (D'Arcy et al., 2009). These should address information security policy, system access control, system development and maintenance, personnel security, physical and environmental security, security organization, asset classification and control, communications and operations management, business continuity management, and compliance (McAdams, 2004).

Maintenance of the smart device GCS is essential for their security. Updates, upgrades, and patches are especially important, as they increase protection from known cybersecurity threats and reduce risks to vulnerabilities in software code in the operating system and software applications. Smart device hardware must also be evaluated and maintained to ensure system effectiveness and ability to meet mission requirements. If the system is deemed ineffective or no longer meets the mission requirements, the devices should be disabled and properly disposed of (Whitman & Mattord, 2010).

To prevent human error or to block compromised personnel from gaining control of the device, controls or safeguards should be implemented. Strong authentication safeguards can be as simple as entering a command twice; having another party verify a command before

> ***If designers are not careful, they can go too far in designing countermeasures and render them more expensive than they are worth.***

implementation; using passwords, smart card, personal identification numbers, and/or a form of biometrics verification (Whitman & Mattord, 2010).

Step 7 – Determine the mitigation plan. In the previous steps, risk was assessed to identify high-priority threats that should be mitigated and countermeasures were identified to block the attacks to the UAV smart device GCS. Once the threat-attacks have been assessed and prioritized, they must be managed by assuming, controlling, transferring, or avoiding the risk. A risk should be assumed if the risk is low and the cost to mitigate is sufficiently high; it can also be transferred to another user via warnings, etc. If a system component or feature associated with a risk is too costly to mitigate or the risk is too high to accept, the risk can be avoided by removing the relevant component or feature. Lastly, a risk can be controlled with countermeasures (Myagmar et al., 2005). If designers are not careful, they can go too far in designing countermeasures and render them more expensive than they are worth. The cost to implement a countermeasure must be factored into the design decision and should not exceed the expected risk (Oladimej et al., 2006).

While cost is an important factor, countermeasures must also be evaluated based on the ability to meet mission goals and offer operational benefits. The UAV smart device GCS is being evaluated for military operations; therefore, countermeasures must enable mission accomplishment with tolerable risk and reflect the environment in which the system is deployed (Clark et al., 2007).

Conclusions

As technology continues to progress, the U.S. government cannot afford to sacrifice security for enhanced capabilities and features on the battlefield. Mission success is always the top priority, but not at the cost of compromising sensitive information, loss of multimillion-dollar assets, or casualties of soldiers. While a number of threat models exist, they have not evolved to effectively evaluate today's technology. Current threat models: (1) focus primarily on software applications, and don't address threats to the system in totality—hardware, software, and communication network, (2) only address the adversary and fail to address the insider threat—users and maintainers of the system, and (3) fail to provide a threat analysis that assesses the risk, prioritizes the threats, and provides countermeasures. The robust threat model we propose

for the UAV smart device GCS has filled the gaps identified in current threat models and has improved on existing techniques by addressing threats to a complete UAS (hardware, software, communication network) and the associated human threats. Our approach also conducts a thorough threat analysis by completing a risk assessment and provides countermeasures for the threats identified. This comprehensive threat model analysis will help designers and users in the military and civilian UAV communities to understand the threat profile of their system and to enhance the security and operational environment of the UAV smart device GCS. Most importantly, the secured devices will provide soldiers with the secure, enhanced mission capabilities needed to protect soldiers in the battlefield.

While this threat model analysis addresses threats to military UAV smart device GCSs, the enhanced threat model can also be used to assess Federal Aviation Administration civilian UAV GCSs and industry applications that use smart devices for the reception and sharing of sensitive information. As technology continues to advance, adversaries will continue to alter their cyber footprint. Governments and industry agencies must adapt accordingly and assess threats effectively. Our model holds the key to the future of security.

References

Alghamdi, A. S., Hussain, T., & Faraz Khan, G. (2010, March). *Enhancing C4I security using threat modeling*. Proceedings of 12th International IEEE Conference on Computer Modelling and Simulation (UKSim) (pp. 131–136), Cambridge, UK, March 24-26.

Bhargava, B. (2013). *Security in mobile networks*. Retrieved from cs.brown.edu/nsfmobile/nsf-contextaware.doc

Bhusari, M. V. K., & Sahu, M. A. M. (2013). Smartphone attacks and security challenges. *International Journal of Computer Science and Management Research*, 2(5), 2473–2476.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *Information Technology, Learning & Performance Journal*, 24(1), 1–14.

Chirillo, J., & Danielyan, E. (2005). *Sun certified security administrator for Solaris 9 & 10 study guide*. Boston, MA: McGraw-Hill.

Clark, J. A., Murdoch, J., McDermid, J., Sen, S., Chivers, H., Worthington, O., & Rohatgi, P. (2007, September). *Threat modelling for mobile ad hoc and sensor networks*. Proceedings of Annual Conference of International Technology Alliance (ACITA) (pp. 25–27), Hyattsville, MD, September 25–27.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79–98.

Delac, G., Silic, M., & Krolo, J. (2011, May). *Emerging security threats for mobile platforms*. Proceedings of the 34th International Convention, MIPRO 2011 (pp. 1468–1473), Opatija, Croatia, May 23–27.

Di, J., & Smith, S. (2007, April). *A hardware threat modeling concept for trustable integrated circuits*. Proceedings of IEEE Region 5 Technical Conference (pp. 354–357), Fayetteville, AR, April 20–21.

Do, T. D., Kwon, J., & Moon, C. J. (2013). Ground system software for unmanned aerial vehicles on android device. *World Academy of Science, Engineering and Technology*, 74, 718–723.

Edwards, J. (2012). *The future of military comms on the battlefield*. Retrieved from http://defensesystems.com/articles/2012/02/08/cover-story-military-communications-technologies.aspx

Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). *A survey of mobile malware in the wild*. Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2011). New York: Association of Computing Machinery.

Goodwin, B. (2013). *IT manufacturers fight cyber espionage risks in the supply chain*. Retrieved from http://www.computerweekly.com/news/2240181320/IT-manfucturers-tackle-cyber-espionage-risks-in-the-supply-chain

Hartman, A. R., Beacken, M. J., Bishop, D. J., & Kelly, K. L. (2011, November). *4G LTE wireless solutions for DoD systems*. Proceedings of the 2011 IEEE Military Communications Conference (MILCOM 2011) (pp. 2,216–2,221), San Diego, CA, November 7–10.

Hasan, R., Myagmar, S., Lee, A. J., & Yurcik, W. (2005). *Toward a threat model for storage systems*. Proceedings of the 2005 ACM Workshop on Storage Security and Survivability. New York: Association of Computing Machinery.

Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. (2012, November). *Cyber security threat analysis and modeling of an unmanned aerial vehicle system*. Proceedings of IEEE International Conference on Technologies for Homeland Security (HST) (pp. 585-590), Waltham, MA, November 13–15.

Jeon, W., Kim, J., Lee, Y., & Won, D. (2011, July). *A practical analysis of smartphone security*. Proceedings of the 2011 International Conference on Human interface (HI '11) and the Management of Information (Vol. I, pp. 311–320), Orlando FL, July 9–14.

Leavitt, N. (2011). Mobile security: Finally a serious problem? *Computer*, 44(6), 11–14.

Lee, W., & Rotoloni, B. (2012). *Emerging cyber threats report 2013*. Retrieved from http://www.gtcybersecuritysummit.com/pdf/2013ThreatsReport.pdf

Lipner, S. (2004, December). *The trustworthy computing security development lifecycle*. Proceedings of IEEE 20th Annual Computer Security Applications Conference (ACSAC) 2004 (pp. 2–13), Los Alamitos, CA, December 6–10.

Markelj, B., & Bernik, I. (2012). Mobile devices and corporate data security. *International Journal of Education and Information Technologies*, 6(1), 97–104.

McAdams, A. C. (2004). Security and risk management: A fundamental business issue. *Information Management Journal–Prairie Village*, 38(4), 36–45.

Mirkarimi, D. B., & Pericak, C. (2003). Countering the tactical UAV threat. US Armor Association, 112(1), 43–44.

Myagmar, S., Lee, A. J., & Yurcik, W. (2005, August – September). *Threat modeling as a basis for security requirements*. Proceedings of 13th IEEE International Requirements Engineering (RE) Conference, Symposium on Requirements Engineering for Information Security (SREIS), Paris, France, August 29–September 2.

Oladimeji, E. A., Supakkul, S., & Chung, L. (2006, November). *Security threat modeling and analysis: A goal-oriented approach*. Proceedings of 10th International Association of Science and Technology for Development (IASTED) International Conference on Software Engineering and Applications (SEA 2006) (pp. 13-15), Dallas, Texas, November 13–15.

Olzak, T. (2006). *A practical approach to threat modeling*. Toledo, OH: Erudio Security, LLC.

O'Rourke, C., & Johnson, S. B. (2011). *Mobile ad hoc networking revamps military communications*. Retrieved from http://www.cotsjournalonline.com/articles/view/102158

Pellerin, C. (2013). *DARPA pioneers tactical mobile devices for soldiers*. Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=121320

Rose, C. (2011). Smart phone, dumb security. *Review of Business Information Systems (RBIS)*, 16(1), 21–26.

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., & Glezer, C. (2010). Google android: A comprehensive security assessment. *IEEE Security and Privacy*, 8(2), 35–44.

Spiewak, D., Engel, T., & Fusenig, V. (2006). *Towards a threat model for mobile ad-hoc networks*. Proceedings of the 5th WSEAS International Conference

on Information Security and Privacy (ISP'06). Stevens Point, WI: World Scientific and Engineering Academy and Society.

Stango, A., Prasad, N. R., & Kyriazanos, D. M. (2009). *A threat analysis methodology for security evaluation and enhancement planning*. Proceedings of IEEE Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2009) (pp. 262–267), Athens, Greece, June 18-23.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Torr, P. (2005). Demystifying the threat modeling process. *Security & Privacy*, 3(5), 66–70.

Troiani, G. (2011). DARPA looking to develop mobile devices to command UAVs. *ExecutiveBiz®*. Retrieved from http://blog.executivebiz.com/2011/12/darpa-looking-to-develop-mobile-devices-to-command-uavs

Varshney, U., & Vetter, R. (2000). Emerging mobile and wireless networks. *Communications of the ACM*, 43(6), 73–81.

Wang, Y., Streff, K., & Raman, S. (2012). Smartphone security challenges. *Computer*, 45(12), 52–58.

Whitman, M. E., & Mattord, H. J. (2010). *Principles of information security*. Boston, MA: Cengage Learning.

Wilcoxson, D. (2013, November). *Advantages of mobile broadband communications services for military applications*. Proceedings of the 2013 IEEE Military Communications Conference (MILCOM 2013) (pp. 266–272), San Diego, CA, November 18–20.

Yin, R. K. (2013). *Case study research: Design and methods*. Thousand Oaks, CA: Sage Publications.

Yochim, J. A. (2010). T*he vulnerabilities of unmanned aircraft system common data links to electronic attack*. Ogden, UT: Weber State University.

Author Biographies

Ms. Katrina M. Mansfield is an engineering management and systems engineering doctoral student at The George Washington University. She has worked for the Department of Defense for the past 7 years supporting operation and integration of avionics devices in naval aircraft. Ms. Mansfield has an MS in Engineering Management from Johns Hopkins University and a BS in Electrical Engineering from Morgan State University.

(E-mail address: kmansfi@gwu.edu)

Dr. Timothy J. Eveleigh is an adjunct professor of engineering management and systems engineering at The George Washington University and an International Council on Systems Engineering (INCOSE) Certified Systems Engineering Professional. Dr. Eveleigh has over 30 years' industry experience working DoD/intelligence community information technology acquisition challenges, research and development, and enterprise architecting. Dr. Eveleigh has enjoyed a 30-year parallel career as an Air Force Reserve intelligence officer and developmental engineer focused on command and control integration.

(E-mail address: eveleigh@gwu.edu)

Dr. Thomas H. Holzer is an adjunct professor of engineering management and systems engineering at The George Washington University. He was the director, Engineering Management Office, National Geospatial-Intelligence Agency, with 35 years' experience in systems engineering and leading large-scale information technology programs. Dr. Holzer holds a Doctor and Master of Science in Engineering Management from The George Washington University and a Bachelor of Science in Mechanical Engineering from the University of Cincinnati.

(E-mail address: holzert@gwu.edu)

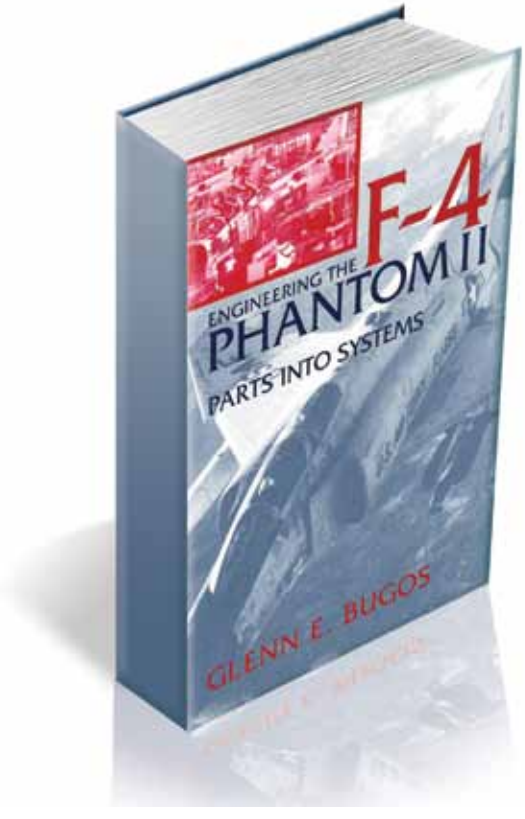
Dr. Shahryar Sarkani is an adjunct professor in the Department of Engineering Management and Systems Engineering at The George Washington University. He has over 20 years of experience in the field of software engineering. Dr. Sarkani holds a Doctor of Science in Systems Engineering from The George Washington University, a Master of Science in Mathematics from University of New Orleans, and a Bachelor of Science in Electrical Engineering from Louisiana State University.

(E-mail address: emseor2003@yahoo.com)

Professional Reading List

The Defense Acquisition Professional Reading List is intended to enrich the knowledge and understanding of the civilian, military, contractor, and industrial workforce who participate in the entire defense acquisition enterprise. These book reviews/recommendations are designed to complement the education and training that are vital to developing the essential competencies and skills required of the Defense Acquisition Workforce. Each issue of the *Defense Acquisition Research Journal (ARJ)* will contain one or more reviews of suggested books, with more available on the *Defense ARJ* Web site.

We encourage *Defense ARJ* readers to submit reviews of books they believe should be required reading for the defense acquisition professional. The reviews should be 400 words or fewer, describe the book and its major ideas, and explain its relevance to defense acquisition. Please send your reviews to the Managing Editor, *Defense Acquisition Research Journal*: *norene.fagan-blanch@dau.mil.*



Featured Book

Engineering the F-4 Phantom II: Parts into Systems

Author:
Glenn E. Bugos

Publisher:
Annapolis, MD: Naval Institute Press

Copyright Date:
1996

Hard/Softcover/Digital:
Hardcover, 258 pages, http://www.amazon.com/Engineering-F-4-Phantom-II-Systems/dp/1557500894

Reviewed by:
Lee Vinsel, Program on Science and Technology Studies, Stevens Institute of Technology

Review:

How can system designers work together and coordinate action across organizational boundaries—often including firms, governments, and universities—and still ensure the resulting product is of the highest quality? It's a question that has plagued systems engineering from the very beginning. In his great book *Engineering the F-4 Phantom II: Parts into Systems*, the historian Glenn E. Bugos draws our attention to this issue and shows how systems engineers have worked to resolve it. No doubt, many readers of this journal will need no introduction to the F-4 Phantom II, a fighter jet produced by McDonnell Douglas. It entered production in 1954 and, within the United States, was retired from service in 1996, ironically the same year that Bugos's book was released.

Production of the jet was complicated, involving the military and several firms, including McDonnell Douglas, General Electric, Raytheon, Westinghouse, Collins Radio, and Lear Instrument. The number of individuals and organizations involved made coordination extraordinarily difficult. Moreover, the Phantom II was re-made several times throughout its long career. As Bugos writes, "The Phantom was built by integrating parts into systems, then disaggregating these systems into smaller parts, and reintegrating them again in different ways." This making, remaking, and rearranging was true not just for the technologies, but also for the organizations involved, many of which went through significant transformations during the technology's lifespan.

Bugos brings the best aspects of the field of science and technology studies to bear on his subject. While he spends a great deal of time and energy spelling out the formal organizational structures that were built to manage the Phantom II, he points out that, really, the most important resource was trust. This focus is probably Bugos's greatest contribution to the literature on systems engineering. Interorganizational cooperation could sometimes break down, leading to hostility and competition. But teams involved in designing and managing the Phantom II created testing practices, verification routines, and other mechanical or quantitative systems of trust-building, which assured that everyone was on the same page and that systems would operate. In practical terms then, Bugos reminds systems engineers that, if they want to be truly successful, they must spend as much care creating healthy interpersonal and interorganizational ties as they do attending to the technical dimensions of their work. It's a lesson worth remembering.

Defense ARJ Guidelines
FOR CONTRIBUTORS

The *Defense Acquisition Research Journal (ARJ)* is a scholarly peer-reviewed journal published by the Defense Acquisition University (DAU). All submissions receive a blind review to ensure impartial evaluation.

IN GENERAL

We welcome submissions from anyone involved in the defense acquisition process. *Defense acquisition* is defined as the conceptualization, initiation, design, development, testing, contracting, production, deployment, logistics support, modification, and disposal of weapons and other systems, supplies, or services needed for a nation's defense and security, or intended for use to support military missions.

Research involves the creation of new knowledge. This generally requires using material from primary sources, including program documents, policy papers, memoranda, surveys, interviews, etc. Articles are characterized by a systematic inquiry into a subject to discover/revise facts or theories with the possibility of influencing the development of acquisition policy and/or process.

We encourage prospective writers to coauthor, adding depth to manuscripts. It is recommended that a mentor be selected who has been previously published or has expertise in the manuscript's subject. Authors should be familiar with the style and format of previous *Defense ARJs* and adhere to the use of endnotes versus footnotes (refrain from using the electronic embedding of footnotes), formatting of reference lists, and the use of designated style guides. *It is also the responsibility of the corresponding author to furnish a government agency/employer clearance with each submission.*

MANUSCRIPTS

Manuscripts should reflect research of empirically supported experience in one or more of the areas of acquisition discussed above. Empirical research findings are based on acquired knowledge and experience versus results founded on theory and belief. Critical characteristics of empirical research articles:

- clearly state the question,
- define the methodology,
- describe the research instrument,
- describe the limitations of the research,
- ensure results are quantitative and qualitative,
- determine if the study can be replicated, and
- discuss suggestions for future research (if applicable).

Research articles may be published either in print and online, or as a Web-only version. Articles that are 4,500 words or less (excluding abstracts, references, and endnotes) will be considered for print as well as Web publication. Articles between 4,500 and 10,000 words will be considered for Web-only publication, with an abstract (150 words or less) included in the print version of the *Defense ARJ*. In no case should article submissions exceed 10,000 words.

Book Reviews

Defense ARJ readers are encouraged to submit reviews of books they believe should be required reading for the defense acquisition professional. The reviews should be 400 words or fewer describing the book and its major ideas, and explaining why it it relevant to defense acquisition. In general, book reviews should reflect specific in-depth knowledge and understanding that is uniquely applicable to the acquisition and life cycle of large complex defense systems and services.

Audience and Writing Style

The readers of the *Defense ARJ* are primarily practitioners within the defense acquisition community. Authors should therefore strive to demonstrate, clearly and concisely, how their work affects this community. At the same time, do not take an overly scholarly approach in either content or language.

Format

Please submit your manuscript with references in APA format (author-date-page number form of citation) as outlined in the *Publication Manual of the American Psychological Association* (6th Edition). For all other style questions, please refer to the *Chicago Manual of Style* (16th Edition).

Contributors are encouraged to seek the advice of a reference librarian in completing citation of government documents because standard formulas of citations may provide incomplete information in reference to government works. Helpful guidance is also available in *The Complete Guide to Citing Government Documents* (Revised Edition): *A Manual for Writers and Librarians* (Garner & Smith, 1993), Bethesda, MD: Congressional Information Service.

Pages should be double-spaced and organized in the following order: title page (titles, 12 words or less), abstract (150 words or less to conform with formatting and layout requirements of the publication), two-line summary, list of keywords (five words or less), body of the paper, reference list (only include works cited in the paper), author's note or acknowledgments (if applicable), and figures or tables (if any).

Figures or tables should not be inserted or embedded into the text, but segregated (one to a page) at the end of the text. When material is submitted electronically, *each figure or table should be saved to a separate,*

exportable file (i.e., a readable EPS file). For additional information on the preparation of figures or tables, refer to the Scientific Illustration Committee, 1988, *Illustrating Science: Standards for Publication*, Bethesda, MD: Council of Biology Editors, Inc. Restructure briefing charts and slides to look similar to those in previous issues of the *Defense ARJ*.

The author (or corresponding author in cases of multiple authors) *should attach a signed cover letter* to the manuscript that provides all of the authors' names, mailing and e-mail addresses, as well as telephone and fax numbers. The letter should verify that the submission is an original product of the author(s); that all the named authors materially contributed to the research and writing of the paper; that the submission has not been previously published in another journal (monographs and conference proceedings serve as exceptions to this policy and are eligible for consideration for publication in the *Defense ARJ*); and that it is not under consideration by another journal for publication. Details about the manuscript should also be included in the cover letter: for example, title, word length, a description of the computer application programs, and file names used on enclosed DVD/CDs, e-mail attachments, or other electronic media.

COPYRIGHT

The *Defense ARJ* is a publication of the United States Government and as such is not copyrighted. Because the *Defense ARJ* is posted as a complete document on the DAU homepage, we will not accept copyrighted manuscripts that require special posting requirements or restrictions. If we do publish your copyrighted article, we will print only the usual caveats. The work of federal employees undertaken as part of their official duties is not subject to copyright except in rare cases.

Web-only publications will be held to the same high standards and scrutiny as articles that appear in the printed version of the journal and will be posted to the DAU Web site at www.dau.mil.

In citing the work of others, please be precise when following the author-date-page number format. It is the contributor's responsibility to obtain permission from a copyright holder if the proposed use exceeds the fair use provisions of the law (see U.S. Government Printing Office, 1994, *Circular 92: Copyright Law of the United States of America*, p. 15, Washington, D.C.). Contributors will be required to submit a copy of the writer's permission to the managing editor before publication.

We reserve the right to decline any article that fails to meet the following copyright requirements:

- The author cannot obtain permission to use previously copyrighted material (e.g., graphs or illustrations) in the article.
- The author will not allow DAU to post the article in our *Defense ARJ* issue on our Internet homepage.
- The author requires that usual copyright notices be posted with the article.
- To publish the article requires copyright payment by the DAU Press.

SUBMISSION

All manuscript submissions should include the following:

- Cover letter
- Author checklist
- Biographical sketch for each author (70 words or less)
- Headshot for each author should be saved to a CDR disk or e-mailed at 300 dpi (dots per inch) or as a high-print quality JPEG or Tiff file saved at no less than 5x7 with a plain background in business dress for men (shirt, tie, and jacket) and business appropriate attire for women. All active duty military should submit headshots in Class A uniforms. Please note: images from Web, Microsoft PowerPoint, or Word will not be accepted due to low image quality.

- One copy of the typed manuscript, including:
  - Title (12 words or less)
  - Abstract of article (150 words or less)
  - Two-line summary
  - Keywords (5 words or less)
  - Document excluding abstract and references (4,500 words or less for the printed edition and 10,000 words or less for the online-only content)

These items should be sent electronically, as appropriately labeled files, to *Defense ARJ* Managing Editor, Norene Fagan-Blanch at: norene.fagan-blanch@dau.mil.

Defense ARJ
PRINT SCHEDULE

The *Defense ARJ* is published in quarterly theme editions. All submissions are due by the first day of the month. See print schedule below.

Author Deadline	Issue
July	January
November	April
January	July
April	October

In most cases, the author will be notified that the submission has been received within 48 hours of its arrival. Following an initial review, submissions will be referred to peer reviewers and for subsequent consideration by the Executive Editor, *Defense ARJ*.

Contributors may direct their questions to the Managing Editor, *Defense ARJ*, at the address shown below, or by calling 703-805-3801 (fax: 703-805-2917), or via the Internet at norene.fagan-blanch@dau.mil.

The DAU Homepage can be accessed at:
http://www.dau.mil

DEPARTMENT OF DEFENSE

DEFENSE ACQUISITION UNIVERSITY

ATTN: DAU PRESS (*Defense ARJ*)

9820 BELVOIR RD STE 3

FORT BELVOIR, VA 22060-5565

Defense Acquisition University

WEB SITE

http://www.dau.mil

Your Online Access to Acquisition Research, Consulting, Information, and Course Offerings

Training

- Apply for Course
- Training Courses
- Continuous Learning Modules
- Certification Standards
- Targeted Training
- Student Policies & Mission Assistance
- Student Information System
- Training FAQs
- Request a Transcript

Other Products

- Mission Assistance
- Knowledge Sharing
- Research Center
- DAU Knowledge Repository & Acker Archive
- Better Buying Power
- Life Cycle Chart
- iTunes
- *Defense Acquisition Guidebook*

iCatalog

- Course Schedule
- Equivalency Fulfillment
- Predecessors/Prerequisites
- Schedules
- Course Material

Publications

- *Defense AT&L Magazine*
- Defense Acquisition Research Journal
- DAU Brochures
- Archived Catalogs
- Annual Report
- Online Publications

Now you can search the DAU Web site and our online publications!

Defense Acquisition Research Journal

S U R V E Y

Please rate this publication based on the following scores:

5 – Exceptional 4 – Great 3 – Good 2 – Fair 1 – Poor

1) How would you rate the overall publication? _____

2) How would you rate the design of the publication? _____

3) Please list all that apply: _____

	True	False
a) This publication is easy to read		
b) This publication is useful to my career		
c) This publication contributes to my job effectiveness		
d) I read most of this publication		
e) I recommend this publication to others in the acquisition field		

4) What themes or topics would you like to see covered in future *ARJs*? _____

5) What topics would you like to see get less coverage in future *ARJs*? _____

6) How can we improve this publication? Provide any constructive criticism to help us to improve this publication: _____

7) Please specify your organization: _____

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 12 FORT BELVOIR,VA

POSTAGE WILL BE PAID BY ADDRESSEE

DEFENSE ACQUISITION UNIVERSITY
ATTN: DAU PRESS
9820 BELVOIR RD STE 3
FORT BELVOIR VA 22060-9910

FREE ONLINE SUBSCRIPTION

☐ *Defense ARJ* *Defense AT&L* ☐

Thank you for your interest in *Defense AT&L* magazine and *Defense Acquisition Research Journal*. To receive your complimentary online subscription, please answer all questions below—incomplete forms cannot be processed.

***When registering, please do not include your rank, grade, service, or other personal identifiers.**

☐ *New Online Subscription*

☐ *Cancellation*

☐ *Change of E-mail Address*

Date

Last Name: _____

First Name: _____

Day/Work Phone: _____

E-mail Address: _____

Signature: (Required) _____

PLEASE FAX TO: 703-805-2917

The Privacy Act and Freedom of Information Act

In accordance with the Privacy Act and Freedom of Information Act, we will only contact you regarding your *Defense ARJ* and *Defense AT&L* subscription. If you provide us with your business e-mail address, you may become part of a mailing list we are required to provide to other agencies who request the lists as public information. If you prefer not to be part of these lists, please use your personal e-mail address.

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 12 FORT BELVOIR,VA

POSTAGE WILL BE PAID BY ADDRESSEE

DEFENSE ACQUISITION UNIVERSITY
ATTN: DAU PRESS
9820 BELVOIR RD STE 3
FORT BELVOIR VA 22060-9910

Defense Acquisition Research Journal

A Publication of the Defense Acquisition University

We're on the Web at:
http://www.dau.mil/pubscats/Pages/ARJ.aspx

Articles represent the views of the authors and do not necessarily reflect the opinion of DAU or the Department of Defense.

Defense Acquisition Research Journal

A Publication of the Defense Acquisition University

Learn. Perform. Succeed.