

Systems Security Engineering: A Critical Discipline of Systems Engineering

Kristen Baldwin, kristen.baldwin@incose.org

In order to adequately address the comprehensive set of threats to its acquisition programs, the United States Department of Defense (DoD) must include systems security engineering as a critical element of systems engineering. Security specialties have emerged over time as responses to new threats and risks; for example, specialties include information security to protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction; physical and personnel security to protect information and other valuable assets physically stored within facilities and installations; and communications and network security to protect electronic information in transit over networks. Security has now become a system-level risk. Twenty years ago, systems were relatively stand-alone, software was critical but not prevailing, and the supply base was known and traceable. Prime contractors build today's complex, software-controlled, highly networked systems by integrating hundreds of suppliers and commercial-off-the-shelf (COTS) components, whose origin and level of integrity are difficult to ascertain. Security vulnerabilities now exist beyond the mitigations that information assurance controls typically provide. They present themselves in embedded software and hardware components and in system-of-systems architecture designs. The discipline of systems security engineering provides an important mechanism for the engineering team to assess and mitigate the vulnerabilities of the system and subsystems. We must grow and resource this discipline and capability.

Call to Attention

For the past several years, the Department of Defense has organized initiatives to focus on security, culminating in 2007 when the Deputy Secretary of Defense declared that the department must “stop the bleeding,” referring to the threat of network attacks on DoD and industry.

We had turned the corner from strategy and planning and moved solidly into implementation.

The journey began in earnest in 2005, when the Office of the Secretary of Defense (OSD) chartered the DoD Software Assurance Tiger Team to focus on the threat of malicious software tampering. Concern had been growing as the production of software had become a global capability. In parallel, the department established a Globalization Task Force, and the Defense Science Board issued two reports recounting the threat, one on microchip supply and one on software. One of the reports summarized the problem in this way:

The Department of Defense faces a difficult quandary in its software purchases in applying intelligent risk management, trading off the attractive economics of COTS and of custom code written offshore against the risks of encountering malware that could seriously jeopardize future defense missions. The current system designs, assurance methodologies, acquisition procedures, and knowledge of adversarial capabilities and intentions are inadequate to the magnitude of the threat. (Defense Science Board 2007)

A System Assurance Strategy

Upon studying the solution space, the Tiger Team issued a DoD Concept of Operations (CONOPS) for system assurance. The team recognized what others had highlighted: that although software is integral to system performance and presents opportunities for tampering, DoD programs must also account for vulnerabilities in the system hardware, firmware, and integration. The team defined system assurance as a measurable attribute of a system:

System assurance is the justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle. (NDIA System Assurance Committee 2008)

The DoD System Assurance Concept of Operations consists of five areas in which to address risk: prioritization (focusing on what is most critical for protection), supplier assurance (better understanding supply chain risk), engineering-in-depth (designing systems with security in mind), industry (gaining industry buy-in to build secure systems), and technology (researching investments to advance our capability to detect vulnerabilities and combat the threat).

The Tiger Team concluded that systems engineering was the core mechanism for implementing the CONOPS. Systems engineering underlies the DoD lifecycle acquisition process, and systems security engineering is a natural means for implementing the CONOPS areas. The following example shows the central importance of systems engineering in the security enterprise. Imagine that the DoD deems a certain system to be critical based upon the potential impact of its loss of integrity or availability on mission success. In addition, a complex weapons platform involves numerous sub-tier suppliers. The government systems engineering team identifies and documents critical information, technology, and components requiring protection. As the engineers develop the system architecture, they perform make-or-buy risk tradeoff analyses for critical components, choosing in-house fabrication where the architecture and design cannot offer enough protection and making commercial purchases where the risk and design allow. The contract references security standards, and systems engineers allocate security requirements to components. Government and supplier engineering teams design, prototype, and evaluate critical components for vulnerabilities, mindful of the security of the integrated system. During and through the end of the engineering design phase, the DoD program manager brings in DoD scientists and engineers to apply techniques to address security requirements, such as anti-tamper features, and

Baldwin *continued from page 11*

to evaluate security using emerging tools and techniques. The program manager then develops and implements plans for secure deployment and sustainment operations, and fields the capability to the warfighter.

State of the Practice

The U.S. Naval Air Systems Command defines systems security engineering in *MIL-HDBK-1785* (1995) as “an element of systems engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities. It uses mathematical, physical, and related scientific disciplines, and the principles and methods of engineering design and analysis to specify, predict, and evaluate the vulnerability of the system to security threats.” Despite this definition and foundation, security is not consistently recognized as a key subdiscipline of systems engineering and therefore is not consistently implemented as part of the systems engineering team’s design, trade, and risk considerations.

There appear to be several reasons why systems security engineering is not routinely a focus in the systems engineering processes used by systems engineering teams in defense and industry. Security is more often associated with information technology and software, as opposed to major weapons systems or their hardware components. This perception has led to gaps in systems science and engineering principles for this discipline, and in guidance and tools for non-information technology solutions. Furthermore, there has been inconsistent identification and enforcement of security as a key system requirement.

The association of security with information systems and software is most likely a result of the current urgent focus and demand for information system security engineers to combat the cyber threat. In industry and government, information system security engineers (ISSEs) are in high demand as the National Security Agency and other organizations combat the emerging cyber threat to information systems. Information systems security engineering is “an engineering process that captures and

refines information protection requirements and ensures their integration into IT acquisition processes through purposeful security design or configuration” (U.S. Department of Defense 2003). Academic engineering departments do not generally include security as a part of their systems engineering curricula, but this is changing; several universities, including Southern Methodist University, now offer degrees in systems security engineering that are associated with the computer science and engineering departments, and several colleges now offer Bachelor of Science degrees in software engineering with a security focus.

It is important for the systems engineering community to understand that information and computer security are but two of the key subdisciplines of systems security engineering. As the DoD Tiger Team concluded, these elements cannot be the sole focus to ensure system security. The standard *ISO/IEC 21827: Information Technology—Systems Security Engineering—Capability Maturity Model [SSE-CMM®]*, identifies the following list of subdisciplines:

- Operations security
- Information security
- Network security
- Physical security
- Personnel security
- Administrative security
- Communications security
- Emanation security
- Computer security

Looking through this list and the associated definitions, it is hard to place the engineering activities that would fully embody the System Assurance CONOPS, or the example implementation that we envision for a complex weapon system.

The Defense Department’s Response and the Way Ahead

In response to a demand for more practical guidance for system security, the National Defense Industrial Association formed a System Assurance Committee in 2006 with the charter to expand the definition of system assurance and clarify its relationship to other important disciplines (e.g., reliability,

information assurance). The committee produced and published the guidebook *Engineering for System Assurance* in fall 2008.

The guide provides two perspectives for systems security engineering. First, it provides an explanation of how criticality analysis and security engineering are integral to the technical and management processes of systems engineering as defined in *ISO/IEC 15288: Systems and Software Engineering—System Life Cycle Processes*. It is hoped that this recognition of security relationships with these processes will lead to the maturing of guidance for systems engineering teams faced with security as a design requirement. The second perspective detailed in the guide is the overlay of security throughout the life-cycle. It is critical for program and systems engineering teams to address security requirements while the largest possible trade space exists, and ensure the technical maturity of the security solution throughout the acquisition life-cycle. We expect that this understanding will also help us with setting and enforcing measures for security.

The publication of this guide is a first step toward motivating the community to adopt systems security engineering as a recognized consideration in systems engineering. Our next steps include updating the content of guidance with experience from pilots and applications. We must also further investigate systems security engineering methods and techniques. One area needing particular attention is verification and validation. We must develop ways to measure and evaluate security, considering component criticality and maturity. There is also a need for tools and techniques to support design for security, such as methods for decomposing systems to identify critical components, architectural approaches to neutralize threats, and ways to optimize life cycle security costs.

Department of Defense policies revised and signed in 2008 reaffirm the requirement to instill protection into our acquisition programs. *DoD Instruction 5200.39: Critical Program Information (CPI) Protection within the Department of Defense* (2008) is the overarching protection policy that sets

forth the requirement to protect “critical program information,” which it defines as “elements or components of an RDA [Research, Development, and Acquisition] program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability.” Critical program information also includes “information about applications, capabilities, processes, and end-items; elements or components critical to a military system or network mission effectiveness,” and “technology that would reduce the US technological advantage if it came under foreign control.”

In the DoD’s *Instruction 5000.02: Operation of the Defense Acquisition System*, the department requires RDA programs to identify critical program information early in the lifecycle as part of a program’s technology development strategy, and requires a program manager to prepare a program protection plan for approval by the milestone decision authority prior to initiation of engineering and manufacturing. The department is now in the process of updating associated guidance, techniques, and tools to assist program teams with these responsibilities.

As described by the defense department, systems security engineering plays an important role in ensuring that our systems function as intended and are free of exploitable vulnerabilities. This threat is challenging and different in kind from the traditional kinetic and capability overmatch threats, or even from nontraditional threats seen in present contingency operations. This information-age threat challenges the engineering community to treat security as a consideration in the risk and design trade space. Given this situation, INCOSE’s decision to charter a working group on systems security engineering is timely and responsive. This decision shows that the international systems engineering community recognizes the importance of security as a key practice in systems engineering. Our community can meet these challenges in several ways: augmenting existing guidance with detailed processes and

tools for our engineering teams; defining core competencies for systems security engineering, and evaluating university curricula against them; setting standards and best practices for key issues such as, How much security is enough?; and assisting program management and resourcing communities to understand the cost and benefit of designing assured, secure systems. As threats evolve, so must our advancements in the field of systems security engineering.

References

- Defense Science Board. 2007. *Report of the defense science board task force on mission impact of foreign influence on DoD software*. Washington, DC: Department of Defense. http://www.acq.osd.mil/dsb/reports/2007-09-Mission_Impact_of_Foreign_Influence_on_DoD_Software.pdf.
- U.S. Department of Defense. 2003. *Department of Defense Instruction 8500.2: Information assurance (IA) implementation*. Washington, DC: Department of Defense.

_____. 2008. *Department of Defense instruction 5000.02. 2008: Operation of the defense acquisition system*. Washington, DC: Department of Defense. <http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf>.

_____. 2008. *Department of Defense instruction 5200.39. 2008: Critical program information (CPI) protection within the Department of Defense*. Washington, DC: Department of Defense. www.dtic.mil/whs/directives/corres/pdf/520039p.pdf.

ISO and IEC (International Organisation for Standardisation and International Electrotechnical Commission). 2002. *ISO/IEC 21827: Information technology—systems security engineering—capability maturity model [SSE-CMM[®]]*.

_____. 2008. *ISO/IEC 15288: Systems and software engineering—system life cycle processes*.

U.S. Naval Air Systems Command. 1995. *MIL-HDBK-1785: System security engineering program management requirements*. Washington, DC: Naval Air Systems Command.

National Defense Industrial Association (NDIA) System Assurance Committee. 2008. *Engineering for system assurance*. Arlington, VA: NDIA. www.acq.osd.mil/sse/pg/guidance.html.

INSIGHT

Preparing Professionals for

INCOSE CSEP Certification

Stockholm, October 21-23, 2009

CSM’s proven Preparation Program available in Europe through Syntell!

Let us support your preparations to become a Certified Systems Engineering Professional (CSEP) in accordance with INCOSE’s certification program in Systems Engineering! In collaboration with the Center for Systems Management (CSM), Syntell organizes a three-day intensive CSEP preparation course, October 21-23, 2009, in Stockholm, Sweden. The course provides a comprehensive walkthrough of INCOSE Handbook version 3.1 which constitutes the body of knowledge for the CSEP certification test.

For more information and registration
training@syntell.se
www.syntell.se



Syntell AB, PO Box 100 22, SE-100 55 Stockholm, Sweden. Tel +46(0)8 660 0280, Fax +46(0)8 660 0965

INSIGHT

INCOSE
International Council on Systems Engineering

July 2009

Vol 12 Issue 2

SPECIAL FEATURE

The Interplay of Architecture, Security, and Systems Engineering



There was a time when architects thought about security... and perimeter defense was sufficient. Systems architects must reclaim the practice. Today, all systems are prey.





INSIGHT

Publication of the International
Council on Systems Engineering

Chief Editor Bob Kenley
insight@incose.org +1 260 460 0054

Assistant Editor Andrew Cashner
andrew.cashner@incose.org

Theme Editor Rick Dove
rick.dove@incose.org

Advertising Editor Christine Kowalski
advertising@incose.org +1 858 541 1725

Layout and Design Chuck Eng
chuck.eng@comcast.net +1 206 364 8696

Member Services INCOSE Central Office
info@incose.org +1 858 541 1725

On the Web <http://www.incose.org>

Article Submission INSIGHT@incose.org

Publication Schedule. *INSIGHT* is published four times per year. Issue and article/advertisement submission deadlines are as follows: *October 2009* issue – 13 August; *December 2009* issue – 15 October; *April 2010* issue – 15 February; *July 2010* issue – 15 May. For further information on submissions and issue themes, visit the INCOSE Web site as listed above.

Advertising in *INSIGHT*. Please see <http://www.incose.org/Products/Pubs/periodicals/advertisinginformation.aspx> – or e-mail advertising@incose.org.

Subscriptions to *INSIGHT* are available to INCOSE members as part of their membership. Complimentary copies are available on a limited basis. Back issues are available on the members area of the INCOSE Web site. To inquire about membership or to order a copy, contact Member Services.

©2009 Copyright Notice. Unless otherwise noted, the entire contents are copyrighted by INCOSE and may not be reproduced in whole or in part without written permission by INCOSE. Permission is given for use of up to three paragraphs as long as full credit is provided. The opinions expressed in *INSIGHT* are those of the authors and advertisers and do not necessarily reflect the positions of the editorial staff or the International Council on Systems Engineering.

Who are we? INCOSE is a 7000+ member organization of systems engineers and others interested in systems engineering. Its purpose is to foster the definition, understanding, and practice of world class systems engineering in industry, government, and academia. INCOSE is comprised of chapters located in cities worldwide and is sponsored by a corporate advisory board and led by elected officers, directors, and membership board.

2008 INCOSE Board of Directors

President: Pat Hale, M.I.T.
President-Elect: Samantha Brown, BAE Systems
Secretary: Bob Kenley, Kenley Consulting, LLC
Treasurer: Ricardo Valerdi, M.I.T.

Director for Leadership and Organizational Development: Bill Ewald, Macro International

Director for Communications: Cecilia Haskins, Norwegian University of Science and Technology

Director for International Growth: Tat Soon Yeo, Temasek Defence Systems Institute

Director for Commercial Outreach: Henk van der Linden, SRON

Director for Strategy: Ralf Hartmann, EADS Astrium GmbH
Corporate Advisory Board Chair: Art Pyster, Stevens Institute of Technology

Member Board Chair: Jonette Stecklein, NASA

Member Board Co-Chair: Richard Grzybowski, Corning

Technical Director: Dick Kitterman, Northrop Grumman

Managing Executive: Holly Witte, Universal Management Services, LLC

Past Presidents

Paul Robitaille, 2006/07	Ken Ptack, 1999	James Brill, 1995
Heinz Stoewer, 2004/05	William W. Schoening, 1998	George Friedman, 1994
John Snoderly, 2002/03	Eric C. Honour, 1997	Brian Mar, 1993
John Clout, 2001	V. A. (Ginny) Lentz, 1996	Jerome Lake, 1992
Donna H. Rhodes, 2000		

President's Corner

STEMming the Coming Crisis in Technical Capabilities

Pat Hale, patrick.hale@incose.org

As those of you who regularly read the “President’s Corner” in *INSIGHT* know, I usually write about matters directly related to our profession of systems engineering or to our organization and its future. I depart from this pattern in this issue to discuss a matter that may gradually, but profoundly, become of critical interest to both our profession *and* our organization: education in science, technology, engineering, and mathematics (STEM).

Many of you know that my “day job” is running a graduate professional program at MIT, concerned with systems design, management, and systems thinking. One of the great joys and opportunities in this job is continually interacting with very bright, professionally experienced students in the program. By virtue of my job as their academic advisor, I have the responsibility of reviewing all program theses to ensure that they meet the goals of the program that I direct. The program requires that “theses must address a topic or topics which contain significant elements of technical and managerial challenges relevant to current industry challenges.” I always enjoy learning about new fields and approaches to solving these relevant industry problems, but one recent thesis in particular captured my attention and provoked a new sense of urgency regarding a problem INCOSE has become increasingly aware of in the past few years, and a problem that profoundly impacts our future professional well-being: the STEM education system.

In his recently completed master’s thesis, Dan Sturtevant (who is now pursuing his doctorate in MIT’s Engineering Systems Division) used system dynamics modeling to explore underlying causes (and potential remedies) of the decline



in STEM subjects and degrees, particularly engineering degrees, among students under 18 (termed “K–12” in the U.S. for “Kindergarten through twelfth grade,” roughly equivalent to ages 5 through 18). Dan drew his data primarily from the U.S., but

compared and related it to non-U.S. data as well. Dan has given me his permission to quote extensively and reproduce data from his thesis in order to illustrate the import and extent of this phenomenon, and I hope to convince you, our members, that this challenge is worth a considerable amount of your attention and energies to create an environment where our “raw material” for systems engineers is nurtured and sustained.

Dan introduces his thesis with this troubling description of the current state of engineering education (Sturtevant 2008, 16):

The percentage of students earning bachelor’s degrees in engineering is almost half what it was in 1985. This decline has occurred despite the fact that wages for engineering graduates are higher than those of any other degree-type. Unemployment for scientists and engineers has just hit a record low. What is being studied in this thesis is an apparent contradiction: people decreasingly willing to go into a field in which wages are extremely strong. On its surface, this situation appears to fly in the face of the law of supply and demand.

The situation is especially bad because a decrease in science and engineering jobs leads to a decrease in the whole state of the economy (Sturtevant 2008, 17):

According to the recent report jointly published by the [U.S.] National Academy of Sciences, National Academy

INSIGHT

International Council on Systems Engineering
7670 Opportunity Road, Suite 220
San Diego, CA 92111-2222

Presort Std
U.S. Postage
PAID
Seattle, WA
Permit #4

What's Inside

President's Corner

STEMming the Coming Crisis in Technical Capabilities 3

INSIGHT Special Feature

The Interplay of Architecture, Security, and Systems Engineering 7

System Security Engineering: A Critical Discipline of Systems Engineering 11

Embedding Agile Security in System Architecture 14

Toward a Dynamic System Architecture for Enhanced Security 18

Resilient Control Systems: A Basis for Next-Generation Secure Architectures 20

Secure Architecture and Design of Component-Based Systems 23

Using the U.S. Department of Defense Architecture Framework to Build Security into the Lifecycle 27

An Architecture of Information Assurance Processes Standardized Practices for Embedding Security from Concept Through Development 33

Balancing Security and Other Concerns within a Systems Architectural Approach 36

Developing a System Architecture for Managing the Nuclear Weapons Enterprise in the Context of a Comprehensive Policy Portfolio 39

Establishing Security Strategy Using Systems Thinking 41

Fellows' Insight

Using Technology to Access a World of Speakers for Chapter Meetings 43

Forum

How to Ruin Your Own Survey and Waste Others' Time 45

Observations of the Resilience Architecture of the Firefighting and Emergency Response Infrastructure 45

Technical Activities

INCOSE Research Plan: 2008-2020 47

A Proposed Road Map for Research in Systems Engineering 49

Report from the 2009 Workshop of INCOSE's Systems Engineering and Architecting Doctoral Student Network (SEANET) 50

INCOSE Operations

Certification Advisory Group Report 53

INCOSE Events

INCOSE Spring 09 56

In Memoriam – John Wisbinski

59

Final Thoughts

61