Editorial of *INSIGHT* Special Issue

Agile System-Security: Sustainable Systems Evolve With Their Environment

Rick Dove, dove@parshift.com

■ **ABSTRACT**

This overview article and the accompanying essays lay groundwork for, and perspectives on, agile system-security guidance for systems engineering. No expertise in security engineering is assumed or necessary to glean systems engineering value. With an agile attack environment, agile system-security is necessary. Agile security is defined as both a resilient (reactive) and composable (proactive) capability to effectively address the unpredictable and ever-evolving environment of adversarial attacker and attack methods – a systems-engineered capability enabled by the system's architecture and design. This definition is agnostic to the type of system, and can encompass information systems, cyberphysical systems, physical systems, enterprise systems, social systems, and military systems. The systems engineering community is addressed with considerations felt necessary for next-generation agile security, enabled by thoughtful systems engineering.

INTRODUCTION

Sustainable systems endure, but only if they evolve in concert with their environment. Relentless technological innovation threatens system relevancy with functional obsolescence. Aggressive adversarial innovation threatens system integrity with functional damage. Both vectors exhibit accelerating trends.

Agile systems, engineered for operational resilience and composability, offer an affordable path to keep pace with these trends. Resilience and Composability (Figure 1) are the two dimensions of systems agility.

Affordability is a function of cost and time, measured as a positive return on investment over system operational life. Designing a system for evolutionary agility may incur some up front design costs otherwise avoided; but extending operational life in this way pays dividends in reduced sustaining costs. Up front evolutionary-design costs can also reduce pre-delivery development costs, enabling affordable mid-development re-direction when initial plans prove inadequate, or the surmised operational environment evolves differently.

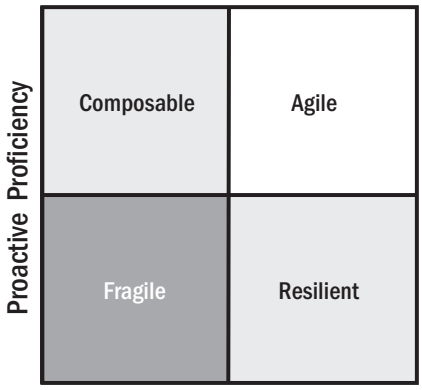

Figure 1. The two dimensions of systems agility

Agility is enabled by a loosely-coupled modular architecture pattern, and facilitated by a sustaining concept of operations (Dove and LaBarge 2014). An agile architecture that enables and facilitates reactive and proactive reconfiguration, augmentation, and evolution mitigates obsolescence in both systems functional components and systems security components. The same architecture mitigates vulnerabilities to purposeful damage of systems integrity in the same way, but facilitating the capability requires new systems engineering thinking, design, and acceptance of responsibility.

This theme editorial and the accompanying articles lay groundwork for, and perspectives on, agile system-security guidance for systems engineering. No expertise in security engineering is assumed or necessary.

ENABLING AGILE SYSTEM-SECURITY

National defense communities recognize the need for resilient and composable systems agility, to counter both obsolescence and security threats. Defense communities are moving in this direction with calls for composable-system architectures and fund-

Insight 19 (2):8-12. International Council on Systems Engineering, July 2016.

ed programs in agile-security initiatives.

Defense contractor Northrop Grumman "is developing composable C4ISR (Command, Control, Communications, Computers, Intelligence, Reconnaissance, Surveillance) systems that allow commanders to best execute their intent. This new generation of highly reconfigurable systems gives them the ability to 'compose' C4ISR assets to respond to and anticipate evolving threats, mission and operations." (Defense Daily 2013).

The United States (US) Department of Defense (DoD) funded Systems Engineering Research Center, in its 2014 Sponsor Review (SERC 2014), recognized a Concept of Operations (ConOps) for systemic assurance that includes system architectural attributes of resiliency and composition quality attributes (Scherlis 2014, 218); and affordability attributes of endurable mission effectiveness, sustainable resource utilization, security protection, modifiable and adaptable flexibility, and open interoperable composability (Boehm 2014, 85).

The US Army Communications-Electronics Research, Development and Engineering Center (CERDEC) outlines their Hardware/Software Convergence initiative: "Develop and mature specifications for a converged architecture during the FY14-17 timeframe. Transition resulting standards to the acquisition community for inclusion in future solicitations and requirements. …Develop a Modular Open RF [Radio Frequency] Architecture (MORA) to support next generation multi-function missions." The approach (Peddicord 2015) employs a classic Agile Architecture Pattern (Dove and LaBarge 2014) with loosely-coupled modules in a plug-and-play infrastructure, shown in Figure 2, and summarized as (acronyms[1]):

- Modular HW and SW subsystems enable timely integration of emerging capabilities while minimizing platform integration issues.
  - Enables tailoring C4ISR/EW capabilities to meet PM needs and platform constraints.
  - Standardizing C4ISR/EW components ensures rapid technology insertion.
  - Facilitates transition and competition across C4ISR component vendors.
- Common HW and SW subsystems enable enhanced C4ISR/EW capabilities to exist within the SWaP constraints of platforms.
  - Commonality across the vehicle fleet reduces lifecycle costs.
  - TRL 7 standards reduce risk to PMs during procurement actions.
- Networked sensors and peripherals, combined with an open modular HW/SW architecture, enables new C4ISR/EW capabilities to be exploited.

1 Acronyms – C4ISR: Command, Control, Communications, Computers, Intelligence, Reconnaissance, Surveillance. EW: Electronic Warfare. HW: Hardware. PM: Program Manager. SW: Software. SWaP: Space, Weight, and Power. TRL: Technology Readiness Level.

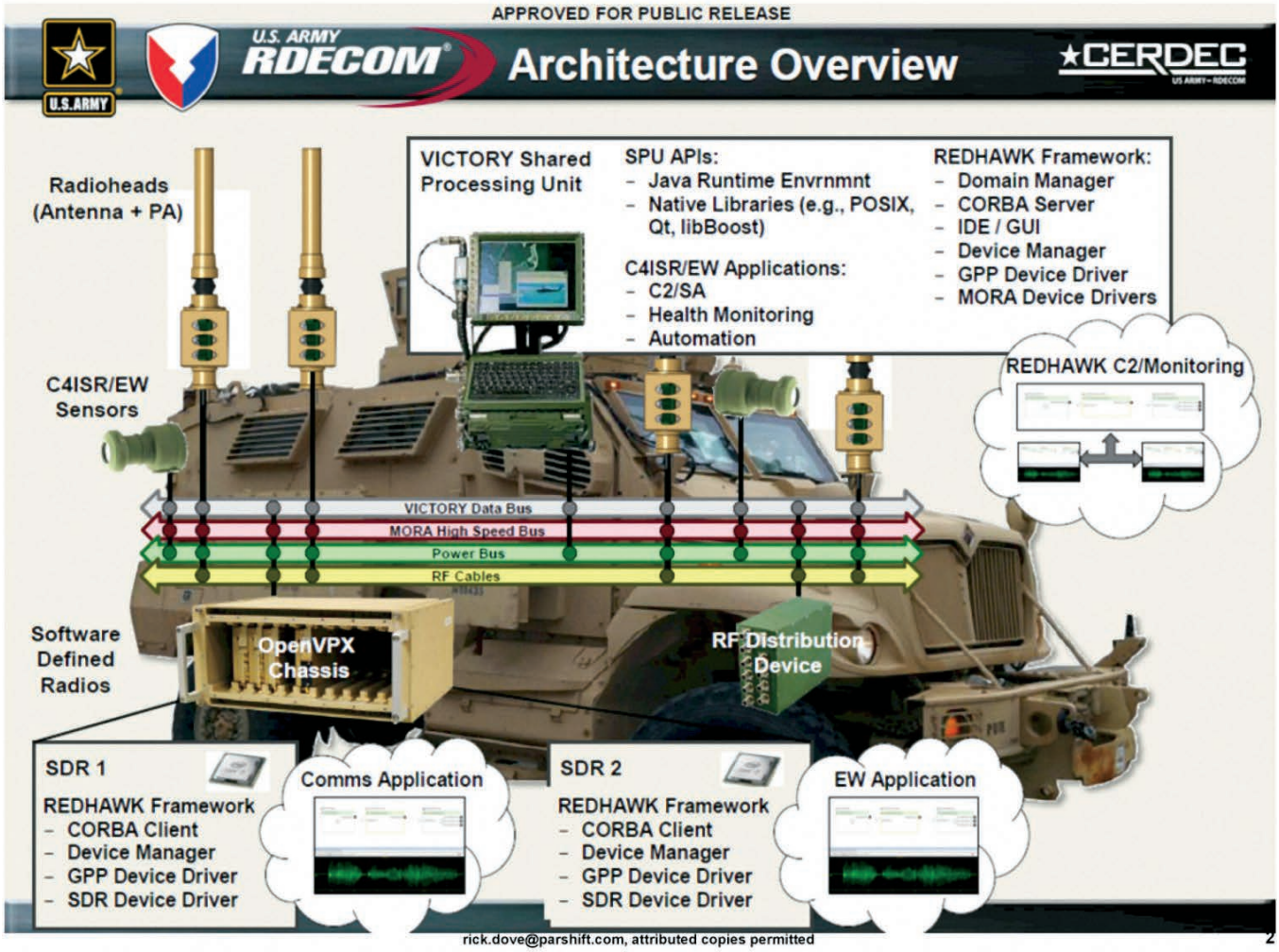

Figure 2. Agility in CERDEC HW/SW convergence initiative enabled with modular technology in a multi-bus plug-and-play infrastructure

- Automated/Dynamic Resource Management.
- Multi-platform Cooperative Capabilities.

The commercial sector employs the Agile Architecture Pattern (Dove and LaBarge 2014) in many ways, perhaps most notably in product line engineering (PLE), sharing components across a family of products, enabled by an architectural infrastructure that facilitates technology insertion and reuse. Note, however, that automotive PLE, for example, shares components across product models and product generations, whereas Google's modular phone project Ara (Computerworld 2016) uses PLE to extend the lifetime of product in current use.

FACILITATING AGILE SYSTEM-SECURITY

Agile security is both a resilient (reactive) and composable (proactive) capability to effectively address the unpredictable and ever-evolving environment of adversarial attacker and attack methods – a systems-engineered capability enabled by the system's architecture and design. This definition is agnostic to the type of system, and can encompass information systems, cyberphysical systems, physical systems, enterprise systems, social systems, and military systems.

There are many active government initiatives pursuing agile security approaches, including (AFRL 2014, DHS 2014, DoD 2011, Herring and Willett 2014, King 2011, Willett 2015). Here we will draw only from a white paper that states the case well: "A healthy cyber ecosystem would interoperate broadly, collaborate effectively in a distributed environment, respond with agility, and recover rapidly. With a rich web of security partnerships, shared strategies, preapproved and prepositioned digital policies, interoperable information exchanges, and "healthy" participants – persons, devices, and processes – a healthy cyber ecosystem could defend against a full spectrum of known and emerging threats. … 'Unhealthy' cyber devices (computers, software, and communications technologies) lack awareness, functionality, or capacity or feature purposeful deceptions. 'Healthy' cyber devices are:

- **Self Aware**. Having the ability to collect information about security properties, draw conclusions, and report or act upon the conclusions.
- **User Aware**. Having the ability to collect or receive and process information about supported users, missions, or business processes or assigned role in a larger cyber infrastructure with the ability to draw conclusions, report or act upon the conclusions, and implement policies that assure user privacy.
- **Environmentally Aware**. Having the ability to collect or receive and process information about the security of surrounding cyber devices of interest or the cyber environment, draw conclusions, and report or act upon the conclusions.
- **Smart**. Having the ability to retrospectively examine events and associated responses, correlate historical patterns with current status data, and either select from a range of ACOAs [Automated Courses of Action] or formulate a new ACOA.
- **Autonomously Reacting**. Having the ability to initiate an ACOA.
- **Dynamic**. Having the ability to alter appearance or persona. Ideally, alterations are enacted on cycle times that are shorter than target acquisition and attack execution times.
- **Collaborative**. Having the ability to work in partnership with other participants to collect and assess security information, and select, formulate, or alter an ACOA intended to counter an attack or sustain priority services.
- **Heterogeneous**. Having the ability to collaborate with other participants using a common communications channel despite differences in affiliation, security policies or service level agreements.
- **Diversifying**. Having the ability to sense the appearance or persona of surrounding devices and to make oneself different from other devices.
- **Resilient**. For cyber defense purposes, having sufficient capacity to simultaneously collect or receive and assess security information, execute any ACOA, make alterations to the ACOA as needed, and sustain agreed upon service levels.
- **Trustworthy**. Performing as expected – and only as expected – despite environmental disruption, user and operator errors, and attacks by hostile parties. (DHS 2011)"

The list above is good, but appears to speak to security engineers. The systems engineering community is addressed in Dove 2009, and 2013, and again below with considerations felt necessary, but unlikely sufficient, for next-generation agile security enabled by thoughtful systems engineering. The intention below is to express these considerations in minimal but concise words, leaving large latitude for how to achieve the intent:

- **Holistic Systems Engineering**. Need: Effective security reconfiguration/augmentation/evolution. Intent: Holistic systems thinking, security embedded in system design as part of system functionality; security system architecture structured and designed for adaptability and evolution.
- **Collective Intelligence**. Need: Collaborative security team. Intent: Knowledge and experience shared and assimilated for organic collective thought and action.
- **Harmony**. Need: Embraceable rather than enforceable security. Intent: Support rather than inhibit human and organizational productivity and goal achievement.
- **Self-Organization**. Need: Response capability at cyber-speed. Intent: Response decision and action automated or human-enabled at the point of maximum knowledge.
- **Consistency**. Need: Eliminate undependable security functionality. Intent: Systemically automated security devoid of reliance on human compliance.
- **Distrust**. Need: Safely employ people and components that change asynchronously over time. Intent: Component-level self-protection that distrusts all interaction.
- **Shape Shifting**. Need: Defeat observation and probing of static system architectures to discover vulnerabilities. Intent: Moving target defense (change functional methods) and offense (evolve capability and functional methods).
- **Component Conscience**. Need: Component self-awareness and evaluation of behavior. Intent: Self-monitoring internal conscience as an embedded independent agent. See Dove 2012.
- **System Conscience**. Need: Awareness of unpredictable emergent system and system-of-systems behavior. Intent: System-wide emergent behavior monitoring by embedded independent agents.
- **Peer Behavior Judgment**. Need: Awareness of aberrant component operational behavior caused by design flaws, system malfunction, human error, and malevolent control penetration. Intent: Peer-peer behavior monitoring. See Dove 2009.

SYSTEMS ENGINEERING GUIDANCE FOR AGILE SECURITY

Though government organizations work agile security concepts into research and development initiatives, without full integration into holistic systems engineering design, these initiatives will not succeed. The articles in this issue of *INSIGHT* are to guide systems engineers in the thinking that will enable and facilitate agile security at a

Insight 19 (2):8-12. International Council on Systems Engineering, July 2016.

systems level. Systems engineering practitioners, some with security backgrounds, and some who simply see the systems engineering responsibility as a necessary part of the solution wrote these articles.

Oh, the Humanity! The Control Side of System Security

Jen Narkevicius, PhD and CEO of Jenius LLC, and Steve Harris, independent Human Factors consultant, tackle the human factors issues of user-friendly security from a control theory point of view.

Enabling Agile Security with MBSE and UPDM

Barry Papke, Director of Professional Services for No Magic, Inc., presents a fundamental agile security architecture, showing enabling roles for MBSE and the Unified Profile for DODAF/MODAF (UPDM).

Critical Infrastructure Challenges

Michael deLamare, Systems Engineering Manager for Bechtel's Nuclear, Security and Environmental business unit; Loren Walker, ESEP and retired VP of Systems Engineering Programs for BCT, LLC; and John Juhasz, CSEP and CEO of Telepath Systems; all co-chairs of INCOSE's Critical Infrastructure Protection and Recovery working group. After outlining some large threats to critical infrastructure, the authors show agile system design principles apply to event recovery.

How Resilience Engineering Maintains Sustainable Value

Scott Jackson, INCOSE Fellow and founder of INCOSE's Resilient Systems working group, provides a foundation for resilience engineering, with design principles for guiding the systems engineer.

A Useful Framework for Security, Resilience and Governance

Marcus Thompson, Brigadier in the Australian Army; and Michael Ryan, PhD and senior lecturer at the University of New South Wales, present a taxonomy for security and argue that sustainable security is ultimately dependent on security-governance agility.

Agile Vetting of Autonomous Systems

Jack Ring, INCOSE Fellow and co-founder of the Autonomous Systems Test & Evaluation working group, explores the challenges in vetting autonomous systems for sustainable system life, and offers a checklist for agile vetting throughout the lifecycle.

ANTS™: A biologically-inspired model for agile cyber defense

Earl Crane, PhD and CEO of Emergent Network Defense, outlines an agile security approach inspired by ants who demonstrate survivability and resiliency in a distributed ecosystem. He argues that organizations managing risks within a risk appetite must move to a dynamic, automated, agile risk management capability.

System-Aware Cyber Security: A Systems Engineering Approach for Enhancing Cybersecurity

Barry Horowitz, PhD and chair of the Systems and Information Engineering Department at the University of Virginia, and Scott Lucero, Deputy Director of Strategic Initiatives in the Office of the Deputy Assistant Secretary of Defense (Systems Engineering) and Program Manager of the Systems Engineering Research Center, review remarkable prototyped project work for system-embedded electronic sentinels, that monitor and detect illogical behavior in system control functions, and restore normal operation when possible.

A Condensed Approach to the Cyber Resilient Design Space

Sharon Norman, PhD, ASEP, and Systems Engineer at Northrop Grumman, and Northrop Grumman coauthors Justice Chase, Daniel Goodwin, William Freeman, Verne Boyle, and Rusty Eckman, describe a cyber security resilience initiative at Northrop Grumman. The article presents two models describing where and how cyber resilience incorporates into systems, with techniques and metrics that can be used to implement and measure cyber security resilience.

System Security Engineering: Whose Job Is It Anyway?

Peri Najib, Northrop Grumman Fellow and Cyber Solutions Architect for the Missile Defense & Protective Systems Division, and Dawn Beyer, PhD and Lockheed Martin Fellow, review an implementation framework tool that guides program protection as the responsibility of an entire systems engineering and systems security engineering team working together.

A Path Towards Cyber Resilient and Secure Systems Metrics and Measures

Holly Dunlap, Sr. Principal Multi-Discipline Engineer at Raytheon and co-chair of NDIA's Systems Security Engineering Committee, observes the confusion arising from different risk evaluation methods in various security specialties, and proposes a method for unifying risk evaluation across these specialties.

Architecting Composable Security

Brian Dōne, Department of Homeland Security; Keith Willett, National Security Agency (NSA); and authors from Johns Hopkins University Applied Physics Lab: Bruce Benjamin, Dan Sterne, Gregg Tally, and David Viel, review the Integrated Adaptive Cyber Defense initiative of the Department of Homeland Security (DHS) and the NSA. This initiative targets the adversaries' ability to execute successful cyber-attacks repeatedly by reusing similar tools and techniques, and removing humans from elements of the incident response loop to speed intervention times.

IN CLOSING

With an agile-attack environment, agile system-security is necessary. The articles in this *INSIGHT* issue draw from practitioners across a broad spectrum of the systems engineering community, who see the need and wish to spur the thinking on agile system-security. In addition to the authors, many helpful reviewers at INCOSE's 2016 International Workshop contributed suggestions for draft article refinements and improved systems engineering relevancy. The effort expended by all testifies to a growing awareness of necessity and urgency. ■

REFERENCES

- AFRL. 2014. BAA-Rik-14-12 2014: Command and Control of Proactive Defense (C2PD). Department of the Air Force, Air Force Materiel Command. www.fbo.gov/spg/USAF/AFMC/AFRLRRS/BAA-RIK-14-12/listing.html.
- Boehm, B. 2014. "Ilities Tradespace and Affordability." In *SERC Sponsor Research Review*, 84-95. Georgetown University Hotel and Conference Center, Washington, US-DC, 25 February. www.sercuarc.org/wp-content/uploads/2014/05/19_SSRR%20 2014_presentations.pdf.
- Computerworld. 2016. Google's Project Ara smartphone project shows signs of life, IDG News Service. 24 March. www.computerworld.com/article/3047690/smartphones/googles-project-ara-smartphone-project-shows-signs-of-life.html.
- Defense Daily. 2013. Open Architecture Summit – Program Guide. Washington, US-DC. 12 November. www.openarchitecturesummit.com/wp-content/uploads/sites/17/2014/03/22859_OA-Program-Guide2013_e.pdf.

continued >

continued from previous page

- DHS. 2011. Enabling Distributed Security in Cyberspace – Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action. 23 March. http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.
- ——2014. Enterprise Automated Security Environment (EASE) Request for Information (RFI). Solicitation Number: RFI201411, Department of Homeland Security. 3 December. www.fbo.gov/index?s=opportunity&mode=form&id=7497164c-010cce00d2f1ce6db79c6727&tab=core&_cview=1.
- DoD. 2011. Department of Defense Strategy for Operations in Cyberspace. US Department of Defense. July.
- Dove, R. 2009. Embedding Agile Security in Systems Architecture. *INSIGHT*, 12 (2): 14-17. www.parshift.com/s/090701Insight-EmbeddingAgileSecurity.pdf.
- ——2012. Righteousness and Conscience as a Path to Socially Acceptable Autonomous Behavior. *INSIGHT*, 12 (2): 14-17. www.parshift.com/s/120701Insight-RighteousnessAndConscience.pdf.
- ——2013. Sustainable Agile Security Enabled by Systems Engineering Architecture. *INSIGHT*, 16 (2): 30-33. www.parshift.com/s/130701Insight-EnablingSustainableAgileSecurity.pdf.
- Dove, R. and R. LaBarge. 2014. Fundamentals of Agile Systems Engineering – Part 1 and Part 2. Paper presented at the Twenty-fourth Annual International Symposium of INCOSE, Las Vegas, US-NV, 30 June—3 July. www.parshift.com/s/140630IS14-AgileSystemsEngineering-Part1&2.pdf.
- Herring, M. J., and K. D. Willett. 2014. "Active Cyber Defense: A Vision for Real-Time Cyber Defense." *Journal of Information Warfare* 13 (2).
- King, S. E. 2011. Cyber S&T Priority Steering Council Research Roadmap, Presentation to National Defense Industrial Association Disruptive Technologies Conference, 8 November. www.dtic.mil/ndia/2011disruptive/King.pdf.
- Peddicord, B. 2015. CERDEC C4ISR/EW Hardware/Software Convergence. http://embeddedtechtrends.com/2015/PDF_Presentations/T07-CERDEC HW-SW Convergence Overview.pdf.
- Scherlis, B. 2014. "Systemic Assurance." In *SERC Sponsor Research Review*, 212-218. Georgetown University Hotel and Conference Center, Washington, US-DC, 25 February. www.sercuarc.org/wp-content/uploads/2014/05/19_SSRR%202014_presentations.pdf.
- SERC. 2014. SERC Sponsor Research Review. Georgetown University Hotel and Conference Center, Washington, US-DC, 25 February. www.sercuarc.org/wp-content/uploads/2014/05/19_SSRR%202014_presentations.pdf.
- Willett, K. D. 2015. Capability-Based Engineering Approach to Integrated Adaptive Cyberspace Defense. Information Assurance Symposium, Washington US-DC, 1 July.

ABOUT THE AUTHOR

Rick Dove is an INCOSE Fellow, and chairs the working groups for Agile Systems and Systems Engineering and for Systems Security Engineering. His is CEO of Paradigm Shift International and an adjunct professor at Stevens Institute of Technology, teaching graduate courses in basic and advanced Agile Systems and Systems Engineering Architecture and ConOps. He leads the current INCOSE project on discovering Agile Systems Engineering Life Cycle Model fundamentals.