Excerpt from INCOSE INSIGHT, Aug 2015, VOLUME 18 / ISSUE 2

Needed: Practitioner Attention to Systems Engineering Delivery of Sustainable Value

Rick Dove, dove@parshift.com

As systems engineers we all want the fruits of our labors to be successful — to be valuable to our customers. Value comes from systems that deliver needed and usable functionality at least long enough to provide a respectable return on investment. We know how to do the business math and calculate the operational life required to justify the investment in an expected and defined system employment environment.

Before a return on investment goes positive, denial or erosion of value can occur. If the systems we use every day to get our jobs done cease to work, that's value denied. If they become less productive, that's value eroded. Value denied can happen for many reasons, which we expect the system designers have anticipated with mitigation preparations. A simple example is the expectation that systems will break occasionally for whatever reason and require service, and the anticipation and provision of the service needs are part of the greater system. All breakage is not complete denial of functionality, as some manifest as reduced effectiveness. We all use email systems, for instance, and have found their functionality and ability to support high productivity degrading over time – more spam to deal with, more restrictions on communication imposed by increasing security concerns.

Systems security is clearly a contribution to sustainable value. Resistance to attack is necessary to prevent denial of value. Resilience under attack is necessary to prevent erosion of value. The challenge is that systems security is not a capability delivered in isolation. It is an integral part of the design and delivery of systems. This article is going to focus on the threat to sustainable value posed by intelligent and determined system adversaries, and suggest that each of our working groups has relevant expertise that needs to come forward.

Three things this article wants to accomplish: 1) show what is necessary to have a better use of systems, 2) show where INCOSE responsibility lies to define and deliver sustainable value, and 3) challenge each working group to contribute in their area of expertise and interest. The July 2016 issue of *INSIGHT* will use system security as the backdrop for a discussion of sustainable value. This does not require security expertise, but it does require the application of relevant knowledge in each working group. The July 2016 issue of *INSIGHT* will offer a way to make that contribution from a practitioner's point of view.

To put the problem in context, the adversary is agile – leading in innovation and adaptability (Dove and Shirey 2010). The only effective countermeasure is an equally agile system security capability. The challenge of *agility* in both threats and safeguards is major, yet remains ignored, or hampered by incompatible systems engineering.

In systems engineering, security is closeted as a specialty engineering process, too easily avoided as a prime functional need. Functionality builds on a presumed foundation of sustainable operation, but security issues undermine that foundation. Sustainable system operational capability is the first functional need. Maslow's hierarchy of needs for organisms recognizes this at the lowest levels as sustenance (food, air, etc.) and safety (Maslow 1943). Only after assurance of existence are higher forms of functional performance considered.

From (Maslow 1943) "*The safety needs.* — If the physiological needs are relatively well gratified, there then emerges a new set of needs, which we may categorize roughly as the safety needs.… The organism may equally well be wholly dominated by them. They may serve as the almost exclusive organizers of behavior, recruiting all the capacities of the organism in their service, and we may then fairly describe the whole organism as a safety-seeking mechanism. Again we may say of the receptors, the effectors, of the intellect and the other capacities that they are primarily safety-seeking tools. … Practically everything looks less important than safety."

The Systems Security Engineering Working Group (WG) by necessity focuses on general system security engineering issues and standards, and cannot bring to bear the focused practitioner's expertise resident in the diversity of INCOSE WGs. All WGs have a responsibility to help address security issues in volatile and evolving systems engineering and systems operational environments.

Some compelling examples follow, and then some guidance for bringing WG expertise to bear on the issues. The intention is to show new needs, show where WG contribution is needed, and sound a call to arms. All systems are finding themselves in new and different environments, vulnerable to unprecedented attack for which our engineered systems are unprepared. If we do not guide the preparation, who will?

RESILIENT SYSTEMS WG

Resilient systems are inherently more secure, yet the fundamentals of resilient

systems have nothing to do with security devices, security software, or security engineering expertise. A resilient system recovers from whatever impedes its functionality regardless of source. System resilience as a security concept is recognized strongly in security circles, but weakly in systems engineering circles. Resilient-systems engineering does not have to be deeply versed in the methods of attackers, but does have to recognize that the malicious intender is succeeding in degrading system performance that manifest as only an intelligent and determined attacker can cause. Resilient design is necessary to build security into the system instead of trying to test it out. This WG has an important opportunity to put some focus on malicious and intelligent system-degradation intent.

ARCHITECTURE WG

Only an architectural design concept that enables both reactive resilience and proactive composability will enable agile security, providing the possibility of at least maneuverable parity with the agile adversary. The Agile Systems and Systems Engineering WG outlined fundamental architectural concepts (Dove 2013; Dove and LaBarge 2014). It is time for the Architecture WG to carry this forward, recognizing that architecture enables or inhibits system security, and providing systems engineering guidance for effective security integration with architecture.

SYSTEMS OF SYSTEMS WG

Systems of Systems (SoS) brings new forms of security concerns. Constituent systems change asynchronously and independently. The concepts of trust need considerable rethinking. Vision 2025 (INCOSE 2014) suggests, "The Internet of Things extends the SoS challenge beyond interconnected computers and users, to include increasingly interconnected systems and devices that monitor and control everything from household appliances to automobiles. … Techniques for analyzing interactions among independent systems and understanding emergent behaviors in SoS must mature and become commonplace."

COMPLEX SYSTEMS WG

The adversarial community is a complex adaptive and self-organizing system, leading in attack innovation by indiscriminately sharing methods, targets, vulnerabilities, attack tools, and resources. The protection community has problems in functioning like an effective community system, and needs a complex systems engineering understanding and approach to solve the requirements and impediments of community-sharing systems.

HUMAN SYSTEM INTEGRATION WG

This is a big one. A major problem with security is that it often has a user interface that impedes personal productivity and organizational goal accomplishment. For instance, everybody's pet peeve: change your password every XX days, make it long and unmemorable, but don't write it down. Therefore, what happens is that people and organizations ignore or otherwise skirt the security requirements when the perception is that these are impediments. It appears that security engineers think more about protective functionality than the realities of usability. Systems engineering must address this with guidance provided by appropriate expertise, but ultimately by reducing reliance on human compliance as a human system integration necessity. The problem in human-system security integration is that we have too much integration and not enough usability. Security expertise needs complimenting guidance from human-system integration expertise.

REQUIREMENTS WG

System security requirements are stuck on compliance with standards and best practices, and need to look more at responsibility, intent, and operational adaptability for future unknown threat vectors rather than inadequate bets on check-off boxes for yesterday's conformance. Here, we need a new approach to requirements, one that speaks to intent and objectives rather than conformance, one that speaks to an environment constantly evolving into unexpected territory. This moves into an area of requirements language that addresses sustainable objectives, recognizing competent best efforts over duplication of best practices. While this WG's Charter scope states "discipline-specific considerations of related areas are avoided," the expansion to dealing with evolving system requirements for evolving environments is not a security-specific need – all system requirements need to consider unpredictable future needs if sustainable functionality is valued. We need to find a way to describe security requirements in the context of time-invariant objectives that define sustainable value.

RISK MANAGEMENT WG

Risk management has a history based on statistical profiles of the past. The risks faced in security keep changing in innovative ways that one cannot evaluate statically or objectively with mathematics at project inception. We need to evaluate systems security design characteristics in the context of risk and not compliance. Systems engineering requires a new fundamental approach for the evolving risk environments our systems cope with today. A new approach should not focus on security alone, as the system's environmental evolution affects all aspect of system risk; but the nature of evolving security risk offers a capability target for establishing new risk assessment requirements, objectives, and methods. Collier (2014) provides the argument supporting a need for new thinking.

CRITICAL INFRASTRUCTURE PROTECTION AND RECOVERY WG

Critical infrastructure is threatened by multiple vectors, from physical destruction to cyber-control intervention. Stuxnet was the wakeup call (INCOSE 2015). Control systems are high-leverage targets of opportunity, from industrial to banking, transportation to healthcare, and defense to offense. To date, INCOSE has no WG focused on control systems. Industrial control systems, for critical infrastructure in particular, are in need of systems engineering perspectives and attention. This WG cannot ignore the Achilles heel of critical infrastructure.

ENTERPRISE SYSTEMS WG

Sony's recent blackmail (Huddleston 2014) and subsequent economic effect appears to have had a nation-state behind it. This event appears to have shaken the security-priority apathy out of many corporate boardrooms. Enterprise IT security strategy is clearly inadequate, and only systems engineering responsibility and attention can change this on a meaningful scale.

INDUSTRY WG

The industry working groups of Automotive and Healthcare should have particular concern in the systems security area. Current automotive security approaches have demonstrated cyber-vulnerabilities, and now come self-driving cars and car-collaborative communications. Security-in-healthcare shortfall is becoming a regular news item, with medical device security gaining increased attention. These problem areas need attention in systems engineering development, to enable security engineers to exercise their expertise.

AUTONOMOUS SYSTEM TEST AND EVALUATION WG

Now here is an area of critical security concern. Autonomous systems with cyber-controls are highly tempting targets of attack. How can you test an autonomous device for something not yet revealed as a threat vector? The testing need is beyond what current test and evaluation best practice and procedure encompasses. Autonomous systems are likely to manifest

emergent behavior. Emergent behavior is necessary, but some will be bad. Without the capability for emergent behavior to be identified and evaluated, such systems will be inadequate in a world of unpredictable situations . We need new test and evaluation approaches for non-deterministic systems.

SYSTEMS ENGINEERING EFFECTIVENESS WG

This WG's Charter states that its "scope is to address the collection, analysis, and distribution of quantitative evidence of the value of SE throughout the system life cycle." Embedding systems engineering responsibility for system security and showing the value proposition doesn't require security expertise. Systems engineering effectiveness is hard to imagine without system-engineered sustainability.

THINGS TO THINK ABOUT WHEN CONSIDERING WG CONTRIBUTIONS

Agile security is addressed here as a system-engineered capability which enables agile systemic behavior. Agile security is both a resilient (reactive) and composable (proactive) capability to effectively address the unpredictable and evolving environment of adversarial attack – a systems-engineered capability enabled by systems architecture and design. This definition is agnostic to the type of system, and can encompass information systems, cyber physical systems, physical systems, enterprise systems, social systems, infrastructure systems, and military systems.

The author feels the considerations listed below are necessary for next-generation agile security, but unlikely sufficient. The intention below is to express these considerations in minimal but concise words, leaving large latitude on how to achieve the intent in guidance contributions from WG expertise:

- 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: Shared knowledge base. Intent: Knowledge and experience shared and assimilated individually for organic thought and action. See Boyd (1987).
- 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. See Kott (2014) for acknowledgement of the need for mixed trust systems.
- Shape Shifting – Need: Static system architecture that one can observe and probe over time to discover vulnerabilities. Intent: Moving target defense (change functional methods) and offense (evolve capability and functional methods). See Horowitz (2012, pages 23-25) for defense.
- Component Conscience – Need: Component self-awareness and evaluation of behavior. Intent: Self monitoring internal conscience as an embedded independent agent. See Dove (2012) and Horowitz (2015, pages 73-105).
- System Conscience – Need: Detection of unpredictable emergent system and system-of-systems behavior. Intent: System-wide emergent behavior monitoring by embedded independent agents.
- Peer Behavior Judgment – Need: Detection 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).

A CALL TO ARMS

The July 2016 *INSIGHT* issue will deal with Agile Security, as a joint leadership effort between the Systems Security and the Agile Systems WGs – but these two WGs do not intend to dominate the contributions. We instead want to engage many WGs in agile-security contributions relevant to their interests and expertise. WGs can contribute by helping to identify the issues relative to their knowledge, and should not try to offer security solutions, but rather sketch what appropriate solutions need to consider from the WG expertise point of view. This can be a systems engineering beginning for the guidance of next generation security. Contact rick.dove@parshift.com with your intent to contribute before the end of September 2015. First draft 2,000 word essays will be due end of November 2015 for open review at an International Workshop 2016 collaborative workshop. ■

REFERENCES

- Boyd, John, 1987. Organic design for command and control. One of the briefings in *A discourse on winning and losing.* Maxwell Air Force Base, AL: Air University Library Document No. M-U 43947. http://dnipogo.org/john-r-boyd
- Collier, Zachary A. Igor Linkov, Daniel DiMase, Steve Walters, Mark (Mohammad) Tehranipoor, James H. Lambert. 2014. Cybersecurity Standards: Managing Risk and Creating Resilience. *Computer*, IEEE Computer Society, September. www.parshift.com/Files/PsiDocs/Paths&MethodsForPeerBehaviorMonitoringAmongUnmannedAutonomousSystems.pdf
- Dove, Rick. 2009. Paths for Peer Behavior Monitoring Among Unmanned Autonomous Systems. ITEA Journal 30: 401–408, September. Best publication of the year award. www.parshift.com/Files/PsiDocs/Pap090901IteaJ-PathsForPeerBehaviorMonitoringAmongUAS.pdf
- Dove, Rick and Laura Shirey. 2010. "On Discovery and Display of Agile Security Patterns." Presented at the 8th Conference on Systems Engineering Research. Hoboken, US-NJ, March 17-19. www.parshift.com/Files/PsiDocs/Pap100317Cser-OnDiscoveryAndDisplayOfAgileSecurityPatterns.pdf
- Dove, Rick. 2012. Righteousness and Conscience as a Path to Socially Acceptable Autonomous Behavior. *INSIGHT* 15 (2): 32-34. International Council on Systems Engineering, July. www.parshift.com/s/120701Insight-RighteousnessAndConscience.pdf
- Dove, Rick, 2013. Sustainable Agile Security Enabled by Systems Engineering Architecture. *INSIGHT* 16 (2): 30-33. International Council on Systems Engineering, July. www.parshift.com/s/130701Insight-EnablingSustainableAgileSecurity.pdf
- Dove, Rick and Ralph LaBarge. 2014. "Fundamentals of Agile Systems Engineering – Part 1." International Council on Systems Engineering International Symposium 2014, Las Vegas, US-NV, 30Jun–03Jul. www.parshift.com/s/140630IS14-AgileSystemsEngineering-Part1.pdf
- Horowitz, Barry (PI). 2012. Security Engineering Project. A013–Final Technical Report SERC-2012-TR-028-2, 23-25. October 24. www.dtic.mil/dtic/tr/fulltext/u2/a582703.pdf

- Horowitz, Barry (PI). 2015. System Aware Cyber Security for an Autonomous Surveillance System On Board an Unmanned Arial Vehicle. Systems Engineering Research Center. Technical Report SERC-2015-TR-036-4 Part 1a, 73-105. January 31. http://serc2cdn1.mannadesignworks.netdna-cdn.com/wp-content/uploads/2014/11/SERC-RT-115-Security-Engineering-Pilot-Final-Report-SERC-2013-TR-036-4-Parts-1a-1b-3-4-20150131.pdf
- Huddleston, Tom, Jr. 2014. The Sony hack should make cyber security a hot boardroom topic. *Fortune Magazine*, December 23. http://fortune.com/2014/12/23/sony-hack-security-boardroom/
- INCOSE. 2014. *A World in Motion – Systems Engineering Vision 2025*. International Council on Systems Engineering. June. www.incose.org/ProductsPubs/products/sevision2025.aspx
- INCOSE. 2015. Cyber Security Considerations in Systems Engineering. *Systems Engineering Handbook 4th Edition*, Section 3.6.4. John Wiley and Sons.
- Kott, Alexander, Ananthram Swami, Patrick McDaniel. 2014. Security Outlook: Six Cyber Game Changers for the Next 15 Years. *Computer*, IEEE Computer Society, 47(12):104-106, December.
- Maslow, A.H. 1943. A Theory of Human Motivation. *Psychological Review*, 50, 370-396. http://psychclassics.yorku.ca/Maslow/motivation.htm