©2020 IEEE – R. Dove and K. D. Willett, "Contextually Aware Agile-Security in the Future of Systems Engineering,"
2020 IEEE Systems Security Symposium (SSS), Crystal City, VA, USA, 1 July-1 August, pp. 1-8,
doi: 10.1109/SSS47320.2020.9174203. https://ieeexplore.ieee.org/document/9174203

Contextually Aware Agile-Security in the Future of Systems Engineering

Rick Dove
Paradigm Shift International
USA
dove@parshift.com

Keith D. Willett
Department of Defense
USA
Keith.Willett@incose.org

***Abstract*—A recurring principle in consideration of the future of systems engineering is *continual dynamic adaptation*. Context drives change whether it be from potential loss (threats, vulnerabilities) or from potential gain (opportunity-driven). Contextual-awareness has great influence over the future of systems engineering and of systems security. Those contextual environments contain fitness functions that will naturally select compatible approaches and filter out the incompatible, with prejudice. We don't have to guess at what those environmental shaping forces will look like. William Gibson famously tells us why: "The future is already here, it's just not evenly distributed;" and, sometimes difficult to discern. This paper provides archetypes that 1) characterize general systems engineering for products, processes, and operations; 2) characterize the integration of security to systems engineering; and, 3) characterize contextually aware agile-security. This paper is more of a problem statement than a solution. Solution objectives and tactics for guiding the path forward have a broader range of options for subsequent treatment elsewhere. Our purpose here is to offer a short list of necessary considerations for effective contextually aware adaptive system security in the future of systems engineering.**

Keywords—FuSE, agile security, cohesion, social symbiosis

I. Introduction

The Future of Systems Engineering (FuSE) is a multi-organization collaborative project with focus on the evolving nature of systems engineering and systems security. The future of systems engineering as an evolution of the discipline will necessarily produce systems that are dynamically attentive and responsive to the environment in which they operate. A system interfaces with and interacts with its operating environment, and remains viable (capable of working successfully) and relevant (appropriate to current desires) only to the extent to which it is operationally compatible with the *current order* of its environment [1]. Environmental factors include shaping forces that define that which is necessary for constituent systems to remain compatible with the environment. A change in environmental shaping forces may require a change in the systems within that environment for those systems to remain viable and relevant; or, in other words, for the system to remain compatible with the environment. One might say that the current order tolerates a clear and present system only to the extent that homeostasis[1] can be maintained or effectively readjusted.

Security is now evolving from a cyber (virtual effects) focus to a cyber-physical system appreciation (virtual and real effects). This is a generally inward view of the system of interest (SoI). There is an important outward looking social dimension to systems that has gone relatively unrecognized beyond the human-social aspect. The social dimension will play a major role in the future of systems engineering, with key implications for system security; i.e., the evolution continues to a *socio-cyber-physical* appreciation that includes people, process, technology, and environment.

The social dimension includes the value of *active collaboration* and *teaming*. Active collaboration brings a diversity of knowledge and thought – of particular relevance when complexity is increasing in both SoIs and their operating environments. Teaming brings faster and more effective action, which is of particular relevance when the adversary is increasingly innovative in method and speed of attack.

Teaming depends on engaged collaboration and includes human and socio-technical teams. For security, teaming includes socio-technical systems collaborating to assure SoI value-delivery via safeguarding the SoI, its function and functional exchanges, and its environment.

The social dimension of systems engineering includes stakeholder *collaborative engagement*, SoI *symbiosis*[2] in a greater System of Systems (SoS), and *compatibility* with the current order. Social aspects for system security include insiders and outsiders as potential system adversaries, adversary social probes, peer behavior awareness and collaboration among interacting systems, and stakeholder personal privacy. Extrospective and introspective awareness and response is both a *systems* (product) and *systems engineering* (process) social aspect in the future of systems engineering.

One aspect of the social dimension of particular interest for security is cohesion – the existence, strength, and dynamics of symbiotic bonds among system elements, both virtual and physical.

[1] Homeostasis: Tendency toward relatively stable equilibrium between interdependent elements. www.lexico.com/en/definition/homeostasis. The sudden appearance of an attacker in the environment is in homeostasis with many systems in the environment that enable/facilitate attack.

[2] Symbiosis: any relationship between different things, people, or groups that benefits all the things or people concerned. www.collinsdictionary.com/us/dictionary/english/symbiosi. Of many, this definition fits our intention.

FuSE recognizes that systems and their environments exhibit emergent behavior (are complex), that systems belong to and are themselves systems of systems, and that the current order and respective constituency are unpredictably dynamic. The dynamics of the current order require security structures and strategies equally dynamic. The adversary is agile, initiating relentless disruptions to the current order and its constituency that requires equally agile security.

What will good look like when FuSE delivers systems security? Security Engineers will be active members of the Systems Engineering team. Security will be rapidly reconfigurable, augmentable, and composable. We will monitor system and component behavior for anomalous behavior. We will use modeling to predict variations and prepare contingent courses of action to be proactive and minimize response time. Security will support rather than impede personal and organizational productivity. System components will be self-protective; e.g., *techno-social contracts* for mutual autonomous protection.

What is stopping us from doing this now? SE relates to security engineering as an independent specialty practice. Security is viewed as a non-functional cost. Stakeholders consider legislative and standards compliance sufficient. Actionable research is in early stages. Functional requirements rather than outcomes drive SE contracting.

This paper provides a relatively succinct foundation for systems engineers to appreciate the needs and intents of security in the future of systems engineering. Objectives herein include to characterize the problem space that shapes the future, suggest considerations for strategies to address the problem space, and outline some next steps for moving toward solutions.

The characterizations and strategies are a short list of *necessary* considerations with no claim of *sufficiency*. System security is not a bounded *logical* entity; rather it is an integrated *structural* and *behavioral* entity distributed throughout a SoI and its environment, where a SoI may be a SoS at any scale.

II. Characterize the Environment

The environment of concern encompasses both external (current order) and internal (value-delivery); and, recognizes both threats (potential loss) and opportunities (potential gain). CURVE is a framework with which to characterize the shaping forces of environments that require an *agile-systems engineering* [3] approach [2]. CURVE is extensible to accommodate the integration of security as part of continual dynamic adaptation.

CURVE characterization of the general SE problem space (Table I column 1 (G-CURVE)) is equally appropriate for the engineered-system (product), systems engineering (process), and the engineered-workflows (operations). The focus of this paper is Table I column 2, the characterization of the system

TABLE I. Environment CURVE Characterization

FuSE General SE CURVE (G-CURVE)	FuSE System Security CURVE (S-CURVE)
Caprice	
1. Survivability (i.e., current order compatibility) 2. Occurrence and nature of emergent behavior 3. Game-changing technologies 4. Availability of symbiotic social relationships	1. Innovative attack and response methods 2. Emergent cascades and complexity effects 3. Artificial intelligence and quantum technologies 4. Collaborative symbiosis
Uncertainty	
1. Relevance (i.e., appropriate to current desires) 2. Cohesion in systems and SoSs 3. Integrity and symbiosis of social relationships	1. Cost vs. value evaluations 2. Operational physical relationships 3. Operational social relationships
Risk	
1. Viability (i.e., capable of working successfully) 2. Cohesion among constituent parts 3. Inadequate recall of lessons learned	1. Design and execution 2. Addressing adversity effectively 3. Knowledge assimilation
Variation	
1. Operational environments 2. Social compatibility 3. Human resource loading	1. Attack and response criticality 2. Peer and community behavior 3. Adequacy of incident response capability
Evolution	
1. More operating environment complexity 2. More SoI complexity 3. Shorter SoI static viability 4. New technology options 5. New malevolent threats to viability 6. Greater social involvement	1. External SoS 2. Internal SoS 3. Growing attack community (skills and scope) 4. Increasing technical innovation 5. Increasing attack value 6. Increasing collaborative connectivity

[3] *Agile-systems* are solutions designed for *continual dynamic adaptation*.

security engineering problem space (S-CURVE), which integrates security into all three aspects. Following the table, we offer a bulleted summary of S-CURVE followed by a discussion of each bullet for the future of system security engineering. The summary is purposefully a short list to encompass the general issues succinctly. Element numbering in each category provide for traceability of derived strategies to the CURVE need.

The goal of integrating security and systems engineering is to sustain SoI compatibility with their environments.

The following is a discussion of the security environment S-CURVE (Table I column 2). Each element in a S-CURVE category is a general concept with many diverse instances under that concept; however, all instances are amenable to general strategy considerations. The sparse examples indicate that the future is already here, with no intent to provide a lengthy set of evidence.

A. Caprice

- **Innovative attack and response methods** are unpredictable with non-deterministic impact on system survivability. Security attack discovery and analysis typically results in fixing known exploited vulnerabilities and augmenting detection mechanisms. This pushes adversaries to continuously find and employ new methods for which there are no safeguards. Resourceful adversaries with interest in high value targets invest significantly to discover and catalogue unexploited system vulnerabilities and await future opportunity. Discovery focuses on both broad infrastructure elements common to many systems (e.g., computer operating systems), as well as peculiarities in more unique systems of interest (e.g., a specific nuclear refinement facility configuration).

- **Emergent cascades [4] and complexity effects** are unpredictable. Increasing system complexity and interconnectedness increases the potential for undesirable emergent cascades; principally an architecture and design issue. Cascades may happen within a system of many components (e.g., 911 World Trade Center collapse), as well as within a system of systems (e.g., Northeast US Blackout of 2003). Undesirable security effects may also occur from unexpected complex interactions of systems within a system of systems.

- **Artificial intelligence (AI) and quantum technologies** have unpredictable employment maturation. AI technology is in its infancy, but evolving rapidly and in early employment by both attacker [3] and protector [4]. Practical quantum computing is an undelivered promise as yet, but a broader spectrum of quantum technologies are much closer to deployed application [5], with quantum key distribution already commercially available. Large budget nation states are actively engaged in a game changing arms race on both the attack and protect side, with trickle down effects as private information is publicly disclosed.

- **Collaborative symbiosis is unpredictable**. This can be a threat when practiced by attackers, and an opportunity when practiced by protectors. In both cases symbiotic collaboration can be unpredictable with the unexpected appearance of new collaborators as well as the failure of existing collaborative relationships. Both attacker and protector can benefit from a larger community of knowledge and awareness. Attackers make use of various internet forums that share newly discovered target values, vulnerabilities, and attack methods. Protectors often exhibit reluctance in sharing information, though there are some closed community forums. Nodes in some ad hoc networks collaborate with each other about suspiciously behaving nodes. Failed symbiotic collaborative relationships for protectors are often issues of changes in priorities, e.g., reallocation of security funding to something considered more important, or the sudden withdrawal of an important collaborative partner that is otherwise engaged on a higher priority need.

B. Uncertainty

- **Cost vs. value evaluations** are uncertain. Security isn't free, nor can it be guaranteed, and objective calculation of value is problematic; yet security is critical to sustain system relevance. Constraints on development and operational budgets often set allocations for security and provide little flexibility in trade-off decisions being in competition with functional and operational priorities. The perception is security is a non-functional cost in the category of *nice-to-have*.

- **Operational physical relationships** are uncertain. During system operation, we may physically remove components for maintenance or replacement. Components may suffer physical damage, or removal by accident or malicious activity. A change in physical relationships protecting components, regardless of cause, may affect security; e.g., protective perimeter structures or anti-tamper mechanisms.

- **Operational social relationships** are uncertain. During system operation relied-upon teaming and collaborative relationships may be impaired. Examples include unavailable critical subject matter experts, obstructed communication channel, otherwise engaged collaborative sources, whimsical employee visitor-badge monitoring.

C. Risk

- **Design and execution** is a risk, whether done by different people or the same person. Done by different people, there is the risk of misinterpreting design intent, assuming design intent is adequate. Done by the same person, there is the risk of insufficient knowledge, experience, and threat evolution awareness to create design intent and execution outcome. In all cases design and execution are at risk from insufficient security appreciation when high level system architecture and design is frozen.

[4] Cascade is something arranged or occurring in a series or in a succession of stages so that each stage derives from or acts upon the product of the preceding.www.merriam-webster.com/dictionary/cascade, last accessed 10-Oct-2019.

- **Addressing adversity effectively** is a risk. Historically, engineers treat security as a non-functional requirement with the objective of satisfying compliance standards. These standards are publicly available and known to the attack community. Compliance standards change slowly, the attack community innovates quickly. Security effectiveness is constrained and enabled by systems engineering decisions made early in the systems engineering process.
- **Knowledge assimilation** is a risk. Assimilation is the process of taking in and fully understanding information or ideas. Systems engineering security decision tradeoffs are based on the assimilated knowledge of decision makers. These decisions are made by the systems engineering team, by business line managers, and by the contracting program manager for contracted systems. In all cases there is a decision risk of competing priorities in the face of insufficient assimilated knowledge.

D. Variation

- **Attack and response criticality** varies. All attacks are not necessarily equally critical, and multiple attacks of different criticalities may occur simultaneously. Evaluating attack criticality establishes response priority. Giving priority to an attack response may be in conflict with achieving other objectives of the moment, e.g., gaining attack knowledge through observation or completing higher priority objectives. Criticality evaluations may change as an attack progresses.
- **Peer and community behavior** varies. The degree of relied-upon human collaborative and teaming engagement can vary in time (e.g., attention limitations, perceived slight). The degree of community compatibility can vary (e.g., degraded communications, new people and systems or components not compatibly integrated as yet, policy changes in systems within an SoS). Emergent behavior (e.g., personality conflicts, contradicting system and component interactions).
- **Adequacy of incident response capability** varies. Overloaded responders. Insufficient knowledge or skills for the immediate response need.

E. Evolution

- **External SoS**. Cyber connectivity, shrinking costs and size, and increased capability fuels growth in systems connected to systems for greater capability delivery. IoT is a current example.
- **Internal SoS**. Cyber-physical systems and components are becoming more complex and incorporating new technologies like AI.
- **Growing attack community**. Part of this growth is due to nation state high quantity staffing; part is due to outsourcing computer jobs to low labor rate countries and then moving those jobs to other countries, leaving jobless computer literates in search of income; part is due to growing computer literacy worldwide looking for skill application opportunities.
- **Increasing technical innovation**. The rate of technical innovation is an exponential curve fueled by knowledge that builds on knowledge.
- **Increasing attack value**. The rise and success of ransom ware and the strategic investments to establish cyberspace as a warfighter domain[5] are two examples.
- **Increasing collaborative connectivity**. DevSecOps is in early stages with a growing focus. Internet tools for remote collaboration are gaining maturity and methods for effective remote teaming approach the tipping point.

The CURVE characterization establishes goals, in the form of a *situational profile* that should have design and operational strategies compatible with the current order. CURVE informs strategy derivation. Strategies to address the CURVEd environment come in two forms, one for *design considerations*, and one for *operational considerations*. The next section will deal with design strategies. A subsequent paper will deal with operational strategies.

III. Design Strategy Considerations

The dynamics of the environment indicate the need for an agile approach to security. We employ a response situation analysis tool as a general framework suitable for our needs [6]. We take minor liberty with this framework to cast it more directly at strategy delineation. We limit our focus to what appears to be necessary strategy with no claim of sufficiency, nor any intent to deal with tactics.

We present design strategies as general concepts without the next level of tactical breakdown; further breakdown is premature until socialization of the general concepts meets with agreement, refinement, or replacement. We enable and invoke agile-security via strategy considerations. We apply agile-security during operations via *dynamic design* (e.g., new modules) and *dynamic composability*[6] (e.g., invoking most appropriate module). Dynamic design and composability activities never end. New threats, new vulnerabilities, and new opportunities emerge throughout the operational lifecycle.

ConOpsCon is a short way to express both ConOps (Concept of Operations) and OpsCon (Operational Concept). ConOps focus is on how the SoI fits with the larger system. OpsCon focus is on the SoI from the stakeholder perspective.

The design-time strategies in Table II are intended to address reference numbered CURVE elements (e.g., C1, U1, etc.) in Table I. The Need (goal) column in Table II identifies strategies intended to maintain and restore compatibility with the system security CURVE characteristics identified in the Intent column of table II.

The framework in Table II has four *proactive* strategy categories, and four *reactive* strategy categories. Proactive

[5] Many consider "cyber war" to be a mischaracterization; i.e., there is only *war* and that through which to engage in war… land, sea, air, space, and cyberspace as the five warfighter domains.

[6] Composable: to make or form by combining things, parts, or elements (e.g., modules); https://www.dictionary.com/browse/composable?s=t

strategies are generally triggered by an opportunity to generate new value in process or product (seek gain). Reactive strategies are generally triggered by a threat to process or product which demands an action (avoid or withstand loss).

TABLE II. DESIGN STRATEGY NEEDS AND INTENTS

Need	Intent (S-CURVE considerations)
Proactive strategies for creating and eliminating	
• Awareness of opportunity and threat • Response actions and options • Assimilated memory • Response action decisions	• All S-CURVE elements • C1, C4, R1 • C1, R3, V3, E1 • C1, V1, E4
Proactive strategies for improving	
• Awareness of design time impediments • Memory in culture, actions/options, ConOpsCon • Action and option effectiveness	• C1, C4, U3, R1 • R3 • C1, V3
Proactive strategies for infrastructure migration anticipation	
• New fundamentally-different types of opportunities • New fundamentally-different types of threats	• E1, E2, E4, E6 • E3, E4, E5, E6
Proactive strategies for modifying capability	
• Actions and options appropriate for needs • Personnel appropriate for needs • Processes appropriate for needs	• C1, C4, R1 • R1, U3 • C4, U3, R3, V3
Reactive strategies for correcting	
• Insufficient awareness • Ineffective actions • Wrong decisions	• C1, C2, V2, V3 • C1, R2, V3 • C4, U1, V1
Reactive strategies for accommodating variable	
• Effective actions and options • Effective evaluations	• All S-CURVE elements • All S-CURVE elements
Reactive strategies for expanding and contracting	
• Capacity for necessary simultaneous activities	• C1, C4, R1
Reactive strategies for reconfiguring	
• Reusable actions • Personnel involved in an activity	• All S-CURVE elements • All S-CURVE elements

A. Proactive creation and elimination

What dynamic design artifacts/data/knowledge must be created or eliminated during design activity? Elimination is a constant pruning activity that expunges obsolete or ineffective elements to minimize bloat and preclude mistaken usage. For creation the distinguishing feature is the development of something new that is not currently present in any modifiable form. Strategies are those that require creation of artifacts.

- **Awareness of opportunity and threat** (all S-CURVE elements): Opportunities to take advantage of and impediments at dynamic design (threats) can happen in virtually any CURVE element. Dynamic design awareness can minimize rework and maximize effectiveness. Consider (highly) a participating role for security engineering on the systems engineering team, and means and instrumentation to monitor dynamic design performance.
- **Response actions and options** (C1, C4, R1): Innovative attacks require the creation of innovative responses, and may require new collaborative partners. Design and development (execution) are creative activities with effectiveness risk. Consider tasks and responsibilities for developing and evolving a knowledge base of possible collaborative resources and techniques.
- **Assimilated memory** (C1, R3, V3, E1): Analyze and document innovative attack methods; document and share innovative response methods for assimilation. Analyze incident response for cause-effect and design-time mitigation. The nature of the evolving external SoS can affect design adequacy in real time, and needs broad assimilation. Consider tasks and responsibilities for memory assimilation in shared stories to enculturate and document in ConOps and OpsCon, and in reusable response methods and attack analysis techniques.
- **Response action decisions** (C1, V1, E4): Enact decisions during operations when time to decision is critical. At dynamic design consider building and maintaining quick-use decision-making trees and/or AI capability to automate or human-assist operational time decision making.

B. Proactive improvement

What dynamic design performance will be expected to improve over time in the design activities? Knowing this can avoid cul-de-sacs in the SE process that impede likely future design-time performance improvement. The distinguishing feature is performance of existing dynamic design activity, not the addition of new activity. Strategies are generally those involving competencies and performance factors, and are often the focus of continual, open-ended campaigns.

- **Awareness of dynamic design impediments** (C1, C4, U3, R1): Dynamic design is generally a team activity. Security engineers have specialty knowledge that can beneficially inform system engineering architecture and design, stay abreast of best practice and innovative security threats and opportunities, bring collaborative resources for special needs, and inform trade off decisions. Consider (highly) a collaborative role for security engineering on the systems engineering team.
- **Memory in culture, actions/options**, ConOpsCon (R3): Dynamic design resources come and go. Design for security never ends as vulnerabilities and threats continue to emerge. New people need to assimilate cultural memory, learn the reusable actions and options, and become familiar with the ConOps/Con. Consider tasks and responsibilities for indoctrinating new people appropriately before their need to perform.
- **Action and option effectiveness** (V1, V3): Effectiveness of actions and options are constrained and enabled by decisions made at dynamic design, by both the systems engineering team and the security action and option developers. The range of incident response options influences action effectiveness; i.e., the correct response to a trigger event. Consider (highly) a participating role for knowledgeable security engineering on the systems engineering team.

C. Proactive infrastructure migration anticipation

What likely events coming down the road will require a change in the design-time infrastructure? Infrastructure includes breadth of human resource capability, policy, and local design-time ConOps and OpsCon. The distinguishing feature is a need to change the nature of the infrastructure beyond simply adding or modifying resources. Strategies are generally those that enable the transition to possible and potential next generation capabilities.

- **New fundamentally-different types of opportunities** (E1, E2, E4, E6): Evolution presents opportunities that may require infrastructure modification. Evolution in the external SoS may offer new potential collaborative partnerships, possible technology sharing among friendlies, and early knowledge of coming threats. Evolution in the internal SoS complexity may reveal emergent behavior good for security. Evolution in technology shortens the grace period for becoming aware of, evaluating, and employing useful new technologies. Evolution in collaborative connectivity with maturing remote collaboration methods may offer effective means for distributed teaming.

  Consider an agile architecture for security dynamic design processes and for security systems that enables affordable and timely infrastructure change; ad hoc briefings to policy makers as evolving opportunities emerge; designated internal or subcontracted responsibilities for monitoring evolution in all opportunity categories; instrumented monitoring of system operation during test and during delivered usage for unexpected emergent security-relevant behavior; early experimental evaluations of promising technologies; distributed remote teaming.

- **New fundamentally-different types of threats** (E3, E4, E5, E6): Evolution presents threats that may require infrastructure modification. Evolution in attack community growth leads to growth in attack methods. Evolution in technology shortens the grace period for becoming aware of, evaluating, and preparing for mitigation of new potential threats. Evolution in attack values changes the attack intents. Evolution in collaborative connectivity leads to a greater shared knowledge base in the attack comminute and more effective attack teaming.

  Consider an agile architecture for security dynamic design processes and for security systems that enables affordable and timely infrastructure change; dynamically scalable design-time security resources; designated internal or subcontracted responsibilities for monitoring evolution in all threat categories.

D. Proactive modification of capability

What modifications to employable resources might need made at dynamic design? The distinguishing feature is a necessary change in available resource capabilities. Strategies are generally those that require something unlike anything already present, or a change to something that does exist.

- **Actions and options appropriate for needs** (C1, C4): Threats evolve beyond what current actions and options can handle, and time is of the essence. Possible and existing collaborative partners come and go unpredictably. Consider an agile architecture that enables the addition of new collaborators, new action options, and the modification of existing action options in minimal time and no side effects; maintain a stable of potential SME collaborators and know the real-time availability of current collaborators.
- **Personnel appropriate for needs** (R1, U3): Design and execution capability has to match emerging and spike needs. Necessary knowledge evolves. Consider reviewing staff knowledge, experience, and capabilities in anticipation of evolving needs; maintaining knowledge of means to augment skills quickly; monitor degree and breadth of assimilated knowledge.
- **Process appropriate for needs** (C4, U3, R3, V3): The evolving environments, both externally and internally, will create needs for modifying the dynamic design systems and security engineering Concept of Operations and Operational Concept, with immediate full team awareness. Consider designated responsibilities for

timely modification of ConOpsCon documentation, and full team indoctrination of changes in both external and internal collaborative partners, knowledge assimilation strategies, and adequacy of incident response strategies.

E. Reactive correction

What will impair/obstruct design-time agility that will benefit from automatic systemic detection? The distinguishing feature is a dysfunction or inadequacy during attempted action. Strategies are generally those that require a recovery from malfunction, recovery from unacceptable side effects, and inability to accomplish a necessary activity.

- **Insufficient awareness** (C1, C2, V2, V3): Attacker innovation, undesirable complex system emergent behavior, dysfunctional peer and community behavior, and inadequate incident response capability can impair the effectiveness of dynamic design activity. Consider proactive monitoring and systemic means for detecting these situations.
- **Ineffective actions** (C1, R2, V3): Innovative attack methods don't have experience-proven protective measures. Addressing agile adversity effectively requires agility in dynamic design actions and options. New protective measures don't have experience-proven incident-response capability. All are trial and error risks. Consider real-time collaborative team evaluations; an agile architecture for security dynamic design processes and for security systems that enables rapid experimentation and recovery from ineffective approaches.
- **Wrong decisions** (C4, U1, V1): Collaborative partners can fail to be there when needed. Security cost vs. value decisions are infrequent, but the environment is not static. Attack and response criticality evaluations occur with available information at decision time, but information changes during attack. Consider continuous monitoring and evaluation of collaborative partners for cost benefit ratio; reevaluating security cost vs. value decisions frequently; an open-ended ability for continuous evaluation of criticality as the environment evolves.

F. Reactive accommodation of variation

What design-time variables will range across what values and need accommodation? The distinguishing feature is predictable variance range but uncertain time of variance occurrence. Strategies are generally those that address variances in resource availability, resource performance, and resource interactions.

- **Effective actions and options (all S-CURVE elements):** There should be a roster of ready-to-use response actions with sufficient options and variations to fit all likely S-CURVE needs. Effectiveness of actions and options are generally variable, as they may not fit a new need optimally, and personnel loading and urgency of response may compromise application effectiveness. Consider procedures for attentive updating of actions and options with lessons learned after every event.
- **Effective evaluations** (all S-CURVE elements): There is an after-action tendency to evaluate the effectiveness of responses to any S-CURVE element on a pass-fail basis. Evaluations that go further can vary in the degree of objective retrospective questioning. Consider having uninvolved third party review and adjudication of evaluations, as ineffective evaluations can be haunting.

G. Reactive expansion and contraction

What are "quantity based" elastic-capacity range needs on resources/output/activity/other? The distinguishing feature is capacity scalability. Strategies are generally those that can be satisfied with planned capacity bounds, as well as those that have indeterminate and unbounded capacity needs.

- **Capacity for necessary simultaneous activities** (C1, C4, R1): At dynamic design there are often conflicts between desired feature development, known vulnerability elimination, and design of emergency attack-mitigation. Consider daily (or as needed) responsible decision-maker involvement in reevaluating or affirming the immediate activity priorities; scalable resource availability.

H. Reactive reconfiguration

What types of resource relationship configurations will need to change during dynamic design? The distinguishing feature is the configuration and employment of available resources. Strategies are generally those that that may have to reconfigure existing resource relationships at dynamic design.

- **Reusable actions** (all S-CURVE elements): All S-CURVE elements have response actions associated variably with awareness, analysis, evaluation, and/or execution. Granular reusable actions may need to be configured into a group appropriate for addressing a particular response need. Consider avoiding or minimizing sequence dependency in action design. The time sequence of granular actions in a group should be reconfigurable as appropriate for the need.
- **Personnel involved in an activity** (all S-CURVE elements): All S-CURVE elements have personnel activities associated variably with awareness, analysis, evaluation, and/or execution. Consider satisfying both need and value in being able to reconfigure the personnel involved in activities for including newly needed skills and for bench depth.

IV. Security as a Functional Requirement

System security engineering is a specialty practice and security engineers traditionally provide comments on system design after its completion resulting, at times, in security add-ons. Stakeholders often perceive security as a non-functional cost; or, a constraint on system functionality rather than an enabler or contributor to functionality. System designs often include security that *adequately* addresses compliance requirements and *sufficiently* protects stakeholders from liability, without truly making the system operationally secure. Integrating security in the system design is more likely to happen when security is part of functional requirements driving the design.

A *functional requirement* for a system is the specification of a required action or activity. The primary functional goal of any system is to *provide value-delivery*; i.e., produce needed results or desired results. Part of a systems functional requirements is 1) the system shall provide value-delivery under nominal conditions and 2) the system shall provide value-delivery under adverse conditions. The latter acknowledges the system may experience a disturbance that induces stress to the system that may affect its ability to deliver value; i.e., there is a functional need not only for value-delivery but also to *sustain value-delivery*. This implies that derived requirements in reliability, sustainability, survivability, resistance, resilience, agility, safety, and *security* that contribute to sustaining value-delivery are themselves functional requirements.

V. Next Steps

This paper provides a foundation for the future system security engineering problem space and general strategies that address the problem space at *dynamic design*. A work in process is similarly developing general strategies for addressing the problem space for *dynamic operations*. We will socialize in the systems engineering and the security engineering communities, and in the FuSE project collaborative community for refinement, augmentation, and concurrence.

After obtaining reasonable concurrence on the problem space, subsequent work will address the solution space, with agile security principles and strategies for employing those principles, measurable objectives, and tactical concepts. Subsequent work will also focus on overcoming barriers to the future of system security engineering that include:

- Systems engineering relates to security engineering as an independent specialty practice.
- Perception of security as a non-functional cost.
- Security compliance is sufficient.
- Actionable research is in early stages.
- SE contracting is requirements rather than outcome proscriptive.

VI. Concluding remarks

This paper instigates thoughts for system security strategies of particular import to *contextually aware agile-security* – and does not attempt a comprehensive treatise on all future considerations.

Key takeaways:

- *Understanding* of the problem space drives the strategy for the solution space.
- Agile security is necessary to contend with agile attack.
- Integrate security engineering into systems engineering.
- System security is a functional requirement.
- Security design and execution is continuous throughout the system life cycle.
- Vigilant awareness of the internal and external process and product environments is essential.
- Knowledge relevant to all stakeholders needs effective assimilation.
- Facilitate action reusability.
- Social interactions among human and non-human system and process resources needs strategy attention.
- Adequacy of incident response is constrained and enabled at dynamic design.
- Systemic behavior and performance monitoring of both process and product will identify problems early.

The future of systems engineering and security will happen whether we see it coming, understand it, or not. Like global warming, its occurrence has nothing to do with our understanding of it. The future of systems engineering will be shaped by the environment and by compatibility with the current order. Natural selection will eliminate those organizations dependent on security approaches that cannot maintain equilibrium with the evolution of the current order.

So why bother with the FuSE project? Though some might think it is to shape and guide the future we want, principally it is because none of us wants to be naturally selected out. We sustain status quo in security engineering by maintaining a solution concept in a problem space it no longer fits. It makes no sense to do this again – so we propose a solution that evolves at the rate of the problem. This takes vigilant awareness of the problem space, and response strategies that can compatibly evolve with the problem space. Also, we are in a time of continuous transformation, and some of us want to drive that transformation, at least to the extent that we have influence on the speed, and perhaps on the steering to the extent that we can minimize the excursions in fruitless directions. For those with no interest in driving, they're on a train with little, if any, control; but might want to know where it's going so they can plan how to enjoy the journey.

The future will happen independent of the FuSE project. Natural selection will be at work. What FuSE offers is early recognition and appreciation for the inevitable, an opportunity to remove barriers and accelerate the coming of the future, and help shape a current order to which we must be compatible.

References

[1] Willett, Keith D. 2019. Systems Engineering the Conditions of the Possibility (Towards Systems Engineering v2.0). International Council on Systems Engineering. FuSE Agility Adaptive Systems Project working paper, August 23.

[2] Dove, R., W. Schindel. 2019. Agile Systems Engineering Life Cycle Model for Mixed Discipline Engineering. Proceedings International Symposium. International Council on Systems Engineering. Orlando, FL, July 20-25. www.parshift.com/s/ASELCM-05Findings.pdf

[3] Stupp, C. 2019. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. Wall Street Journal. August 30. www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

[4] Capgemini Research Institute. 2019. Reinventing Cybersecurity with Artificial Intelligence - The new frontier in digital security. Report 20190711 V06. www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf

[5] Wallden, P., E. Kashefi. 2019. Cyber Security in the Quantum Era. Communications of the ACM, Vol. 62, No. 4. Pp 120-129. April. https://cacm.acm.org/magazines/2019/4/235578-cyber-security-in-the-quantum-era/fulltext

[6] Dove, R., R. LaBarge. 2014. Fundamentals of Agile Systems Engineering – Part 1. International Council on Systems Engineering, International Symposium, Las Vegas, NV, 30Jun-3Jul. **www.parshift.com/s/140630IS14-AgileSystemsEngineering-Part1.pdf**