Frameworks for Analyzing and Developing Agile Security Strategies - Oriented for the Energy and Utility Sector

by Rick Dove, rkdove@AgileSecurityForum.com
Agile Security Forum, www.AgileSecurityForum.com

The unified Agile Security Analysis and Development Framework consists of six framework tools, three for analyzing cyber-security situations and three for designing fit cyber-security solutions. These six framework tools have initial profiles that will be tested, augmented, and refined by employing them in collaborative knowledge-development exercises. These exercises will identify and analyze open problems at participating organizations, analyze candidate existing solutions for effectiveness and rational characteristics, and design rational fitness criteria for solutions that address the open problems. The objective is to transform these initial six framework tools into effective tools uniquely focused on the design of rational security strategy - that demonstrates lower risk, lower vulnerability, higher trust, increased reactive response, and new proactive response - leading to more effective security at lower security-related costs.

Participating organizations seek to illuminate and rectify any misalignment of internal security strategies with the dynamics and nature of uncontrollable reality. To accomplish this, we adapt some existing framework tools that arose from agile systems and enterprise research, and refine some proposed framework tools based on research in decision-making behavior, bounded rationality, and systems engineering science.

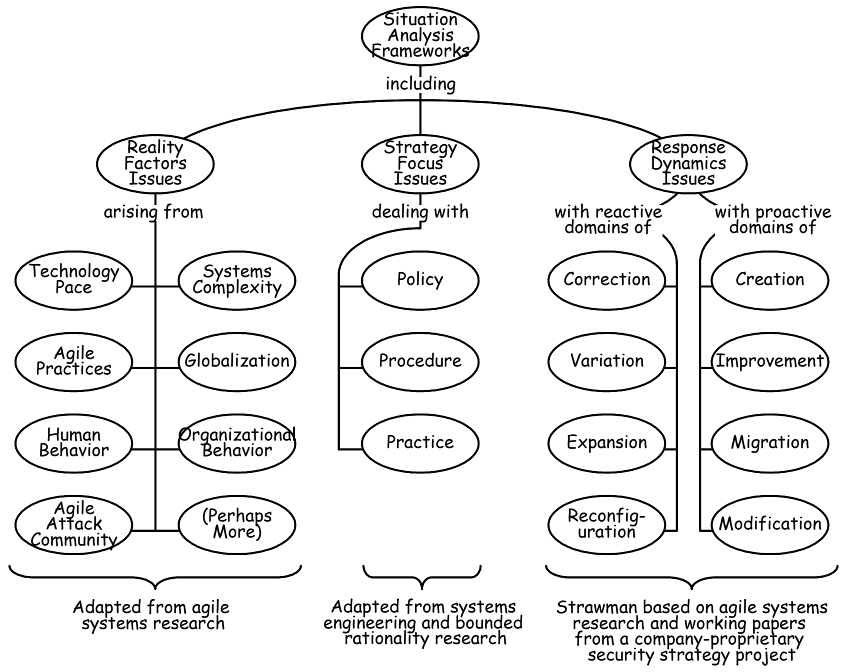
The elements of the six framework tools are outlined below, with their origin, status, and scientific basis noted.

Situation-Analysis Framework Tools

The three analysis framework tools are 1) the Strategy-Focus Issues Framework, for focusing the analysis on each of the three elements of security strategy, 2) the Reality-Factors Issues Framework, for structuring nature and impact analysis of seven reality-issue focus areas, and 3) the Response-Dynamics Issues Framework for structuring identification and requirements analysis of four proactive and four reactive situation-dynamic domains.

Strategy-Focus Framework - Security strategy in the large consists of policies, procedures, and practices. This framework provides analysis focus on each of these three elements. They encompass the totality of security strategy and are based on the three typical functional categorizations familiar to organizations. As the three categories do not share universal definition from one organization to another, the framework offers precise definitions for use in analysis activities. No expansion in categories is expected, but definitions may undergo some refinement.

This is a map summarizing concept relationships.
Relationships are read downward along connecting lines.



Situation-Analysis Framework Tools

1. Policies are organizationally approved objectives. They typically manifest as a controlled document, augmented often with undocumented tacit organizational and cultural understandings. They include principles governing general and contextual expectations, regulatory compliance, level of acceptable risk, desired human behavior, and tradeoffs between quality of service and security needs.
2. Procedures are organizationally approved methods. They typically manifest as a controlled documents, augmented often with undocumented tacit organizational and cultural understandings. They include controls and process methodologies.

3. Practices are organizationally intended executions of policies and procedures. They manifest as configured and deployed network infrastructure protections, security appliances, security software and security services; and, importantly, actual human task-performance activities.

Reality-Factors Framework - Human and organizational decision making behavior is key, and is informed by the research of Simon [1], Cyert and March [2], Kahneman and Tversky [3], and Dove [4]. The origin of this initial framework is a work-in-process to define a cross-industry Agile Security Forum initiative [8]. This initial framework is expected to undergo considerable refinement and perhaps some augmentation if additional categories surface during the project.

1. Agile practices - including outsourced IT, outsourced business processes, and electronic interconnects with energy suppliers, energy brokers, co-generators, demand-response customers, automated meters, SCADA field assets, and wireless-linked field personnel.
2. An agile attack community - Ashby's Law of Requisite Variety demands that a response system be at least as agile as the environment that creates the need for response. The demonstrated agility of the attack community far surpasses that of the defender.
3. Natural human behavior - security strategy impacts individual productivity and goal priorities. In so doing, it is often ignored or circumvented in actual daily decision making and practice - purposely, whimsically, vengefully, and in error.
4. Natural organization behavior - security strategy impacts organizational productivity and goal priorities. In so doing, strategy is often inadequately designed and deployed, and often purposely suspended or circumvented.
5. Increasing globalization - interconnecting with and acquiring technology and services from people of different cultures with different values and practices presents real mismatch in both expectation and practice.
6. Increasing pace of new-technology - replacing and upgrading the IT infrastructure brings incompatibilities and problems discovered in the proving grounds of new and unpredictable usage modes.
7. Increasing complexity of systems - inevitable as networks grow and interconnect on larger scales, and as network nodes, hardware and software alike, grow in sophistication. Unanticipated consequences *are* the consequence.

Response-Dynamics Framework - Agile systems research [5, 6] provides this framework for analyzing a problem in terms of its dynamics. The project will adapt this framework to the specifics of Electric Utility security agility. The framework structures change into two general categories: reactive changes that are responses to demanding external events, and proactive changes that are internally initiated with intent.

Reactive change subcategories include:
1. Correction: Rectify a dysfunction. Issues are generally involved with the failure to perform as expected, recovery from malfunction and side effects, and the rectification of a problem.
2. Variation: Real-time operating change within the mission. Issues are generally associated with operational activity, performance and interaction variances which must be accommodated.
3. Expansion/Contraction: Increase or decrease of existing capacity. Issues are generally involved with quantity and capacity changes, when either more or less of something is demanded or desired.
4. Reconfiguration: Reorganize resource or process relationships. Issues are generally involved with the reconfiguration of existing elements and their interactions, sometimes with added elements as well.

Proactive change subcategories include:
1. Creation/Elimination: Create something new or eliminate something that exists. Issues are generally involved with the development of something new where nothing was before, or the elimination of something in use.
2. Improvement: Incremental improvement. Issues are generally involved with competencies and performance factors, and are often the focus of continual, open-ended campaigns.
3. Migration: Foreseen, eventual, and fundamental change. Issues are generally associated with changes to supporting infrastructure, or transitions to next generation replacements.
4. Modification: Addition or subtraction of unique capability. Issues are generally involved with the inclusion of something unlike anything already present, or the removal of something unique.

Solution-Fitness Framework Tools

The three solution-fitness framework tools are: 1) the Agile Design Principles Framework, for guiding solution design architecture with ten agile-systems principles, 2) the Objectives Framework, for structuring the elements of a specific security-solution strategy into six proactive and six reactive domains, and 3) the Excellence Principles Framework, for maximizing effectiveness consistent with three systems engineering principles adapted for security systems.

Agile-Design Framework - Research [5, 6] on design principles for agile systems provides this ten-element framework. Augmentation of framework categories is not expected as they represent general principles that have been tested and proven in a wide variety of agile systems analysis and development. Descriptive refinement within categories is expected as principles are tailored specifically for security application during the project.

This is a map summarizing concept relationships.
Relationships are read downward along connecting lines.

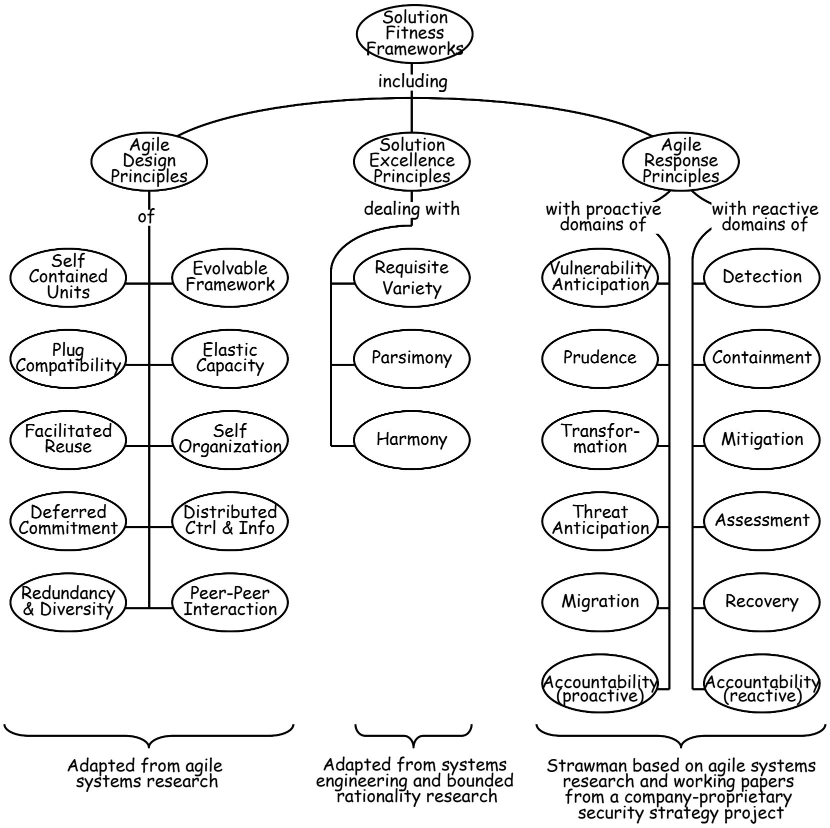

Solution Fitness Frameworks
including
Agile Design Principles
of
Self Contained Units
Evolvable Framework
Plug Compatibility
Elastic Capacity
Facilitated Reuse
Self Organization
Deferred Commitment
Distributed Ctrl & Info
Redundancy & Diversity
Peer-Peer Interaction
Solution Excellence Principles
dealing with
Requisite Variety
Parsimony
Harmony
Agile Response Principles
with proactive domains of
with reactive domains of
Vulnerability Anticipation
Prudence
Transfor-mation
Threat Anticipation
Migration
Accountability (proactive)
Detection
Containment
Mitigation
Assessment
Recovery
Accountability (reactive)
Adapted from agile systems research
Adapted from systems engineering and bounded rationality research
Strawman based on agile systems research and working papers from a company-proprietary security strategy project

Figure 4 – Pathfinder Initiative – Solution-Fitness Framework Tools

1. Self-Contained Units (Modules) - Components are distinct, separable, self-sufficient units cooperating toward a shared common purpose.
2. Plug Compatibility - Modules share defined interaction and interface standards; and are easily inserted or removed.
3. Facilitated Reuse - Modules are reusable/replicable; and responsibilities for ready re-use/replication and for management, maintenance, and upgrade of module inventory is specifically designated.
4. Evolving Standards (Framework) - Frameworks standardize inter-module communication and interaction; define module compatibility; and are monitored/updated to accommodate old, current, and new modules.
5. Redundancy and Diversity - Duplicate components are employed to provide capacity right-sizing options and fail-soft tolerance; and diversity among similar components employing different methods is exploited.
6. Elastic Capacity - Module populations may be increased and decreased widely within the existing framework.
7. Flat Interaction - Modules communicate directly on a peer-to-peer relationship; and parallel rather than sequential relationships are favored.
8. Deferred Commitment - Module relationships are transient when possible; decisions and fixed bindings are postponed until immediately necessary; and relationships are scheduled and bound in real-time.
9. Distributed Control and Information - Modules are directed by objective rather than method; decisions are made at point of maximum knowledge; information is associated locally, accessible globally, and freely disseminated.
10. Self-Organization - Module relationships are self-determined; and component interaction is self-adjusting or negotiated.

Agile-Response Framework - By expressing the requirements of a strategy, and each of its constituent elements, in terms of a fitness function, proposed solutions can be filtered for acceptability before specific features are weighed against competing alternatives. This framework is an initial strawman adapted generally from agility research [5, 6] and subsequently augmented specifically for an agile-security-strategy working paper at a semiconductor foundry [9]. This is an untested framework that is expected to undergo considerable refinement and augmentation during the project.

Reactive Principles
1. Detection – Detect intrusion and damage quickly
2. Containment – Minimize potential damage scope
3. Mitigation – Minimize potential damage magnitude
4. Assessment – Understand what has been damaged and how
5. Recovery – Repair damage quickly
6. Accountability (Reactive) – Identify the perpetrators forensically, after damage

Proactive Principles

1. Vulnerability/Risk Anticipation – Identify pending changes to vulnerability and risk before occurrence
2. Prudence – Correct vulnerabilities before exploitation, sense indirect indicators of pending exploitation
3. Transformation – Change randomly the elements/nature of security system
4. Threat Anticipation – Identify and counter threats and risks before exploitation
5. Migration – Continuous upgrade of security strategy and components
6. Accountability (Proactive) – Identify perpetrators with traps, glass houses, disinformation, etc, before damage

Solution-Excellence Framework - This framework is an initial strawman based on research in systems engineering [7] and research in bounded rationality [1]. During the project this framework may undergo some augmentation with additional categories, and is expected to undergo considerable refinement and descriptive expansion specific to security excellence within categories.

1. Requisite Variety - Provides functional quality by observing Ashby's Law: "The larger the variety of actions available to a control system, the larger the variety of perturbations it is able to compensate....variety must match variety."

2. Parsimony - Leverages Occam's Razor to arrive at the simplest effective solutions and reduce unintended consequences.

3. Harmony - Provides aesthetic quality by engendering user knowledge, trust and respect, principally by supporting rather than inhibiting human and organizational productivity and goal priorities.

Conclusion

Knowledge frameworks are not a new concept. The emphasis here, however, is on the development of insight for design principles and analysis considerations - attempting to make it second nature and alter the way people think about and see problems and appropriate solutions. Also new here are the specific frameworks for security systems - which must be agile because of the agility of the attack community and the ad hoc implementation of agile operating practices. New too is the addition of excellence principles, and especially the principle of Harmony. The focus on human and organizational behavior is also new, as is the solution-fitness concept directing the use of design principles to be employed.

If the resultant requirements analysis is used for an RFQ, this enables objective and innovative solutions. If used for internal problem understanding, it characterizes the recognition of acceptable off-the-shelf solutions, provides an evaluation procedure that maintains a high degree of objectivity, and can drive internal development programs with full audit trail on requirements justification.

As experience is gained in framework application they will undoubtedly evolve. Experience in the past leads us to expect that the evolution will not be radical, but bear a strong similarity to the procedure and initial frameworks, as they are based on effective prior work.

References

1 - H.Simon, *Administrative Behavior*, Free Press; 4th edition, 1997
2 - R.Cyert and J.March, *A Behavioral Theory of the Firm,* Blackwell Publishers, 1992.
3 - D.Kahneman and A.Tversky (Editors), *Choices, Values, and Frames,* Cambridge University Press, 2000
4 - R.Dove, *Value Propositioning - Perception and Misperception in Decision Making,* Iceni Books, 2005, www.parshift.com/ValueProp/VPBook1.htm
5 - R.Dove, *Response Ability - The Language, Structure, and Culture of The Agile Enterprise,* Wiley, 2001
6 - Agility Forum, Lehigh University, various publications, 1991-1996.
7 - International Council on Systems Engineering (INCOSE), various publications, www.incose.org.
8 - R.Dove, "Pathfinder Initiative - Concept of Operations", Agile Security Forum, www.AgileSecurityForum/Docs/AsfPaperConceptOps.pdf
9 - R.Dove, "MyFab Security Strategy – Concepts, Supporting Policies, and Procedures", Silterra Inc., proprietary working paper, April 2002

Rick Dove

Rick Dove is CEO of Paradigm Shift International and Chairman of The Agile Security Forum. He was educated as an electrical engineer at Carnegie-Mellon University, did graduate work at UC Berkeley toward a PhD in Computer Science, spent his early career as a systems software developer, and gravitated quickly to start-up, turn-around, and change management. He has run companies producing software products, manufacturing machinery and services, strategic planning and management services, and fine wine production. He has led engineering, R&D, IT, information security, sales, and marketing in a variety of companies. He co-patented the world's first electronic postage meter. He's created, organized, and led project consortia from proposal through operating phases with NIST, DARPA, and NSF funding, for clients such as Lockheed-Martin, Rockwell Rocketdyne, Collins Avionics, and Texas Instruments. He's interfaced with

Navy, Air Force, DLA, and NIST program managers. He developed and led the National Center for Manufacturing Science's first R&D agenda, and designed and implemented its consortia collaborative procedures. He initiated the US involvement in the international Intelligent Manufacturing System consortia program. He orchestrated the Department of Defense support for the agile enterprise program at Lehigh University, was co-principle investigator on its seminal formation project, and led the subsequent Agility Forum research and industry involvement activity funded by DARPA through Navy and NSF channels. He went on to organize and lead independent collaborative projects that identified and developed design principles for agile systems in general. He is co-author of *The 21st Century Manufacturing Enterprise Strategy*, and author of *Response Ability: The language, Structure, and Culture of the Agile Enterprise* and *Value Propositioning - Perception and Misperception in Decision Making*.