International Council on Systems Engineering
A better world through a systems approach

Systems Engineering with Attitude

Enchantment Chapter, 12-Nov-2025

Rick Dove

This work is part of the FuSE Security Project in the Systems Security Engineering Working Group

Collaborators: Rick Dove, Mona Humes, Greg Leach, Richard Massey, Gerry Ourada, Barry Papke, Adam Scheuer, Martin Span, Daniel Sudmeier, Luke Thomas, Adam Williams, Beth Wilson, Mark Winstead – with acknowledgement to Gary Stoneburner

Systems Engineering with Attitude

IS25 Paper: http://www.researchgate.net/publication/394312045

Abstract

This presentation covers material in INCOSE's *Systems Engineer's Security Primer*—which outlines the role of systems engineering in creating perseverant systems—ones designed to endure and prevail in an environment of constantly evolving, intelligently-directed, predatory hostility. Security, as a collection of intents, methods, and techniques, has attempted improvement by broadening and extending a legacy mindset. This approach is failing. Outlined here is a new mindset and approach that aligns with, and is enabled by, systems engineering principles. This material forms the substance of an in-process INCOSE Systems Engineers Security Primer.

Presenter Bio

Rick Dove is a Fellow of the International Council on Systems Engineering (INCOSE), chairs the working groups for Agile Systems and Systems Engineering and for System Security Engineering, and leads the projects for System Security in the Future of Systems Engineering and for Agility in the Future of Systems Engineering.

Bottom Line Up Front

Paper's purpose is background for a pending 4-page primer.

Goal: Give SEs an embraceable direction and role in the systems security equation – systems perseverance in a hostile predatory environment.

Strategy: Create a useful and simple mental model of what should be done for who and why.

- Rational appeal: can be accomplished with current SE skills applied with a new focus.
- Emotional appeal: Personal orientation in a 4-page quick read.

Objective: SEs headed in a rewarding direction with a good attitude and mission, engaging with an evolving systems engineering experience.

Some thinking people want security to be as fundamental to systems engineering as safety and performance.
We thought that was a good think – but a straight forward attack kept running into it-won't-happen-here.
A dozen SEs and SSEs decided a different approach was needed.

Calling It Like It Is

Predatory hostility is an active characterization of a system's operational environment.
Damage, disruption, and destruction are the intended or ransomed outcomes.

Complexity of attack and defense continuously increases
as iterative incremental attack evolution
makes yesterday's defense approach insufficient and obsolete.

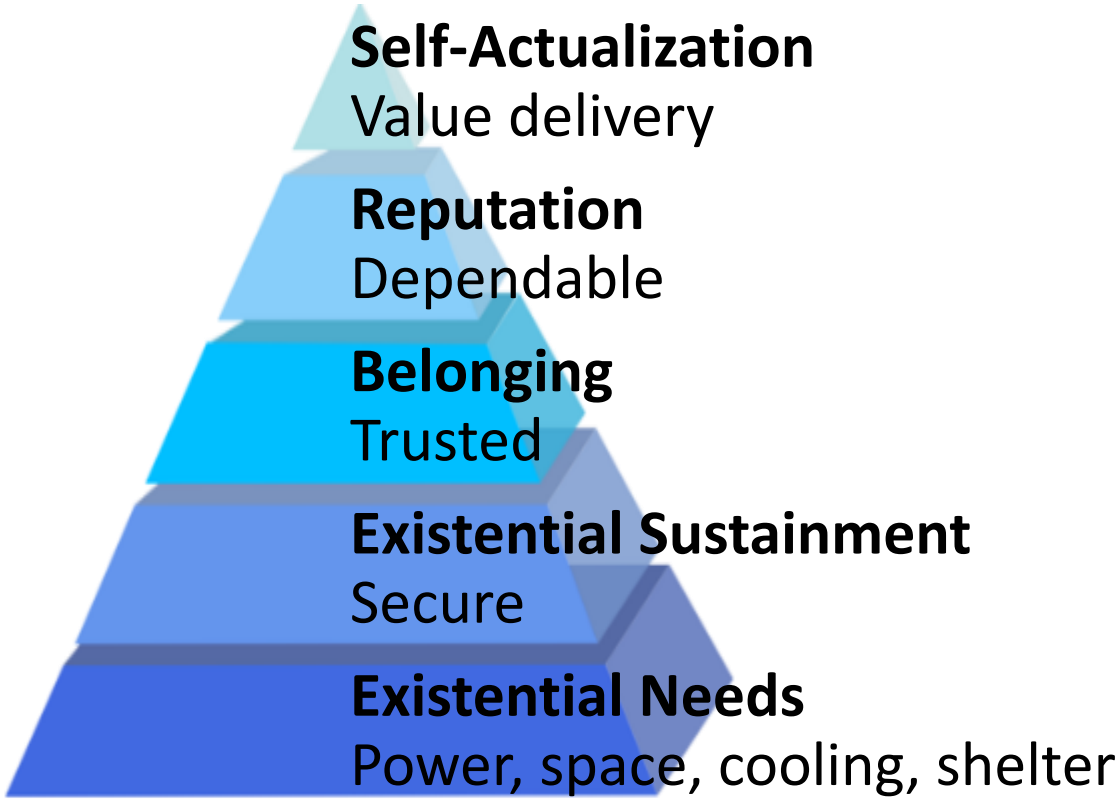
Predatory hostility is not new activity,
but featuring it as the bottom-line issue
can change the way we think and deal with it.

Adopting a Different Point of View

It’s not about security (the means)

It’s about stayin’ alive (the outcome)

Stayin' Alive is a Prerequisite of System Functionality



Technical Hierarchy of Needs

Adaptation of Maslow's Hierarchy of Needs

Context

Systems engineering was conceived and defined for the industrial environment.

The digital environment is demanding change:

- **Model based systems engineering.**
- **Agile systems engineering.**
- **Digital systems engineering.**
- **Systems engineering's role in the security equation.**
- **Artificial intelligence impact on, and for, systems engineering.**

Competing for attention is best done
by minimizing the amount of attention required.

Perseverance

Continuing to make an effort to do or achieve something, even when this is difficult or takes a long time.

What is the role of systems engineering in creating perseverant systems …

ones made to endure and prevail in an environment of constantly evolving, intelligently-directed, predatory hostility?

Reactive knowledge, methods, and techniques are not working.

We need a systems-based mindset and doctrine, compatible with systems engineering.

"It's a list of possible side effects."

The Perseverance Point of View

- … is not about security (a means),
  it is about staying alive (an outcome).

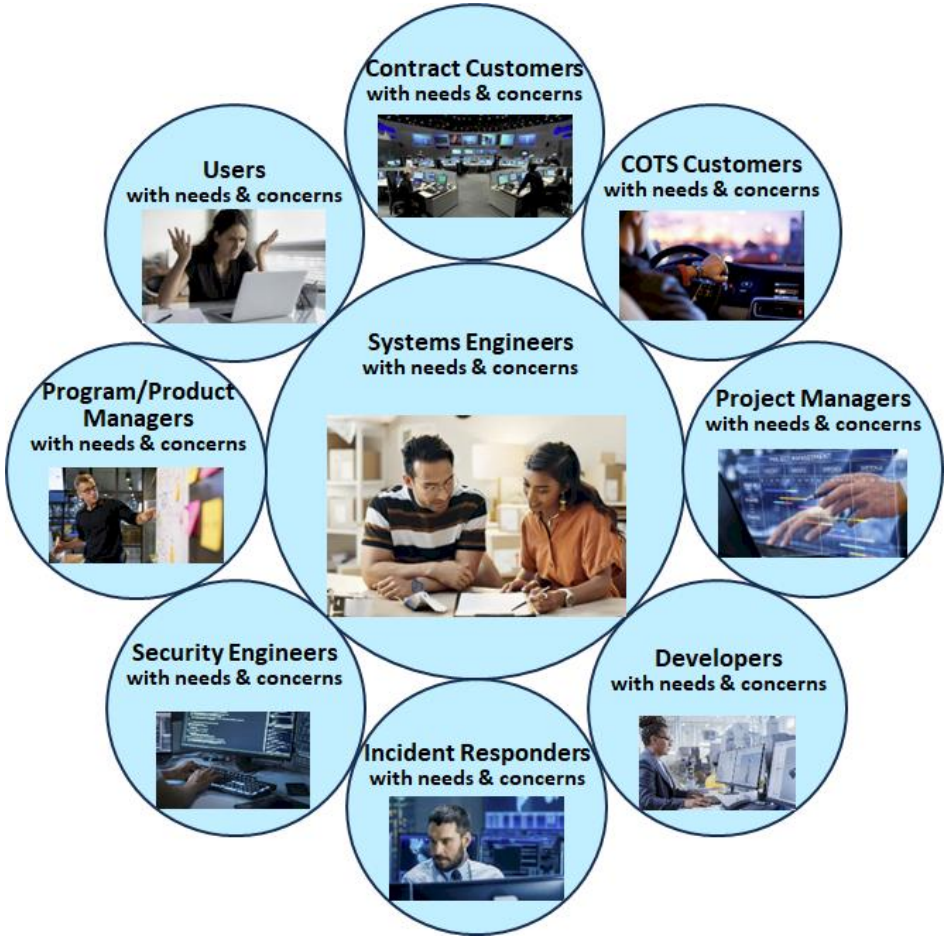
- … is not about being everyone's job (making it no one's job),
  it is about being a team sport (with a role for every player).

- … is not about security engineers (protectors and defenders),
  it is about systems engineers
  (setting objectives, weighing tradeoffs, coaching team play).

- … is not about the system (a constructed object),
  it is about the constituency that serves and is served by the system
  (an organic group of dependents).

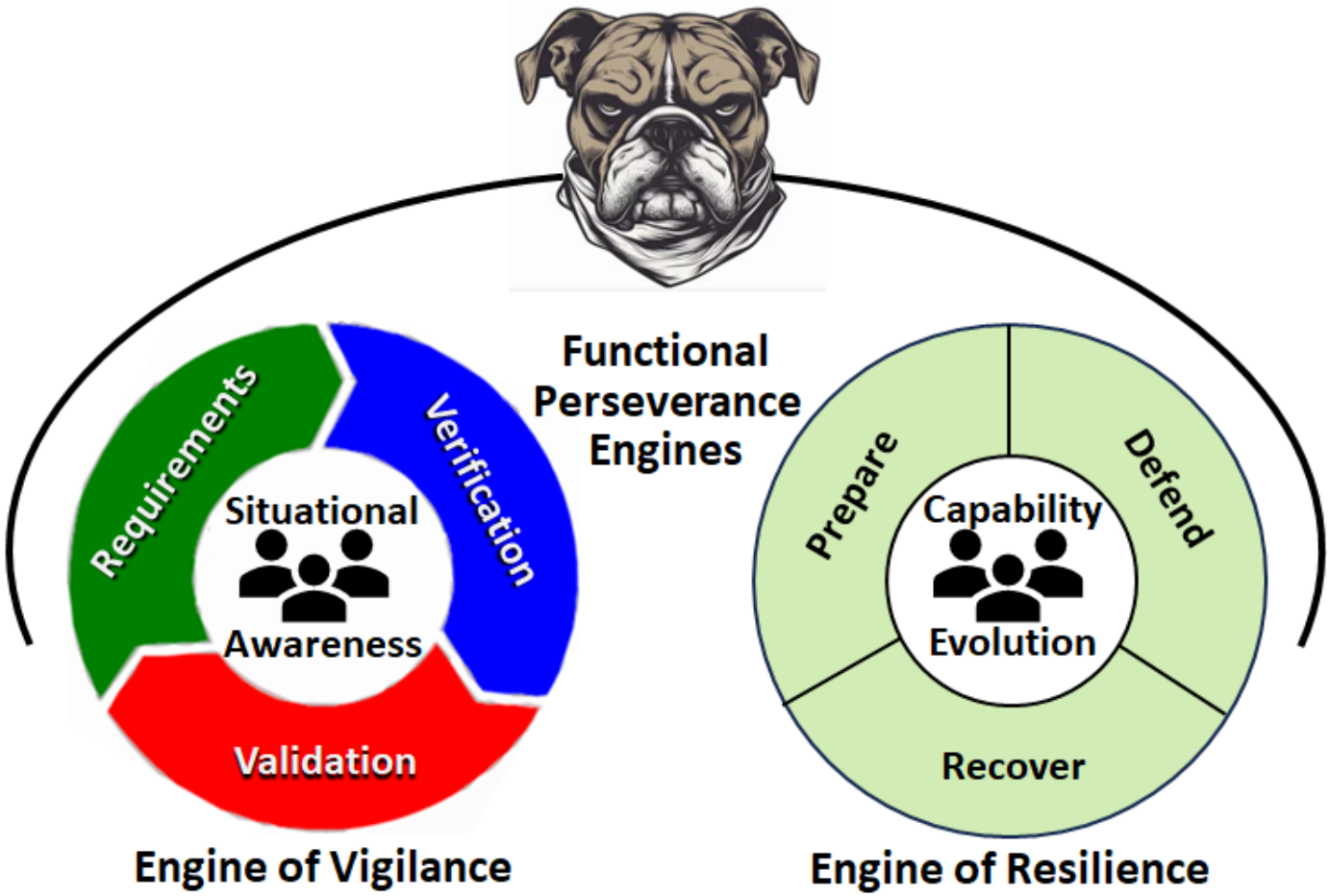
Representative Sampling of Constituent Needs and Loss Concerns

Constituent	Needs	Loss Concerns
Users	Easy/seamless security; knowledge of role & response options; …	Availability; predictable trustworthy behavior; …
Contract Customers	Short-lived adverse behavior; cost effective verification/certification; …	Value delivery; mission success, organizational reputation; …
COTS Customers	Trustworthy operation; convenient to keep secure; …	Dependability; functionality; …
Program/ Product Mgrs	Satisfied owners/users; SE security champion; …	Acquisition satisfaction; budget and schedule performance; …
Project Managers	Comfort with security mission; knowledge of personal role; …	Personal reputation; costly delays; …
Developers	Knowledge; productivity; design requirements; …	Personal and product reputation; rework; …
Security Engineers	Early collaboration with systems engineering; meaningful requirements; …	Professional respect; ability to influence system perseverance; …
Incident Responders	Situational awareness; historical data; fallback; containment; recovery/restoration; …	Personal reputation; operational ownership; system functionality; behavior visibility; …
Systems Engineers	Knowledge of constituent's needs and loss concerns; …	Personal and product reputation; system functionality; …



The Engines of Perseverance

Mindset: Hostile Predatory Environment
Doctrine: Functional Perseverance
Attitude: Self Preservation



Engine of Vigilance

**Vigilance keeps careful watch for potential dangers,
pays close attention to emerging threats,
is driven by active situational awareness.**

Requirements – Needs oriented, loss-driven, capability-based security requirements.
Common sense is required, not security expertise.

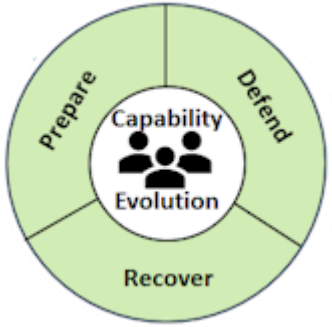
Verification – A fundamental systems engineering skill.
Close-the-loop due diligence that all required capabilities are in fact present.

Validation – In a static sense this is a quality issue—are requirements sufficiently comprehensive.
In a dynamic sense this is a time-based issue—has the situation changed?

Awareness – Doing the right thing is a moving target, and validation is a perpetual activity.
Situational awareness as a functional activity should be perpetual throughout life cycle.

Engine of Resilience

**Resilience is driven by evolution,
enabling capability innovation across three time frames:
before, during, and after a confrontation event.**



Prepare – **Preparation includes development and employment of technology, and leverages security education, coaching, training, and response exercises.**

Defend – **Incident response is inevitable and the active part of system perseverance. Facilitating incident response is preferable to paying ransom or killing a rogue system.**

Recover – **Capabilities can run the gamut from slow repair to instant replacement, and can lean on emerging understandings from systems resilience engineering.**

Evolve – **Security mechanisms evolve or the system ceases to be viable. Capability evolution as a functional activity should be perpetual throughout the life cycle.**

What's New?

Systems engineering has always addressed endurance.
This is not a new concern. However, what is new includes:

- **Predatory intelligence**
- **Systems as targets**
- **Accessible system controls**

What's Newish?

- Perseverance requirements engineering
- Systemic situational awareness
- Systemic capability evolution
- Coaching constituents in their security roles
- Emphasis on Resilience

What's Not?

- Systems Engineering
- Requirements Engineering
- Verification and Validation
- Team Coaching

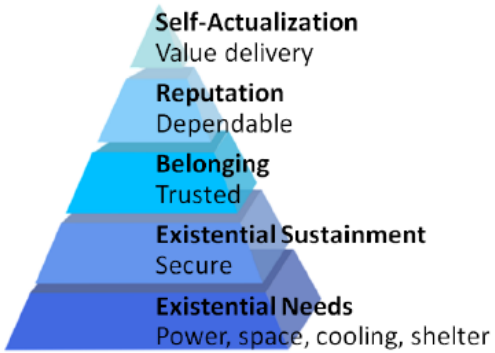
Systems Engineer's Security Primer

Existential threats to systems have escalated with the ease of access brought by the digital age. Functional perseverance has become a prerequisite requirement of systems performance. This primer orients existing SE skills for a compatible role in the systems security equation, with a life cycle focus and model of what should be done for whom and why.

This primer outlines the role of systems engineering in creating perseverant systems—ones with resilient system capabilities and enduring mission relevance in environments of constantly evolving, intelligently-directed, predatory hostility. Outlined here is a mindset and doctrine aligned with, and enabled by, systems thinking and systems engineering.

Security is a prerequisite of functionality

A technical adaptation of Maslow's hierarchy of needs illustrates that fuel and security are the first two existential needs for a system and serve as prerequisites of all higher-level needs. Robotic mobile devices, for instance, will interrupt tasks to seek an electrical outlet when power runs low, and your computer operating system will cease to service you when an intrusion is detected.



Technical Hierarchy of Needs,
an adaptation of Maslow's Hierarchy of Needs

Calling it like it is.

Predatory hostility is an active characterization of a system's operational environment that eclipses passive characterizations that use words like threat, adversary, and cyber contested environments. Damage, disruption, and destruction are the intended or ransomed outcomes.

Complexity of attack and defense continuously increases as iterative incremental attack evolution makes yesterday's defense approach temporal and insufficient.

Evolving Perspective

System security (often instantiated through regulatory compliance), standards adherence, and best practices, has attempted improvement by broadening and extending a traditional protective mind set. That's no longer working. The nature of predatory hostility evolves constantly, outpacing systems not explicitly designed to evolve —a term that shifts the emphasis from security engineering (as a means) to systems engineering (as an overarching objective).

Mindset and Doctrine

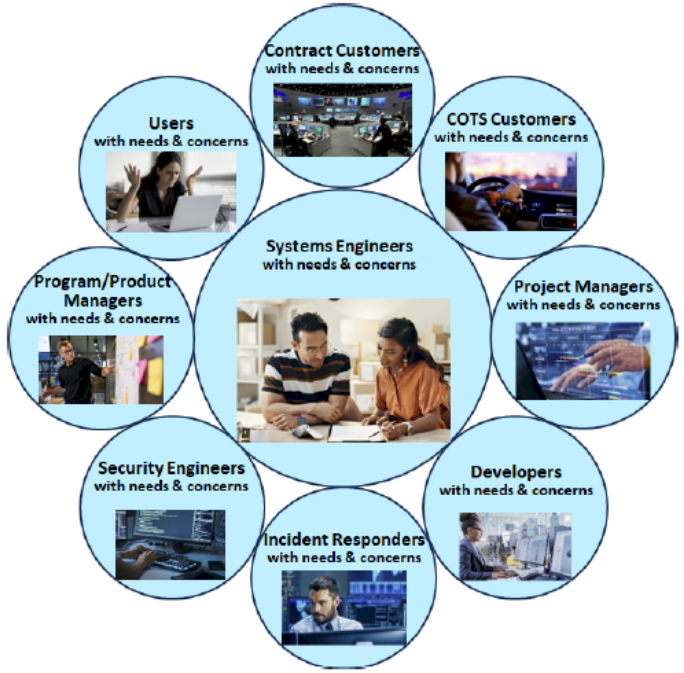
Mindset is a way of thinking, often expressed as an attitude or opinion, a dominant viewpoint that shapes and governs the interpretation of, and interaction with, events and situations. Doctrine is a statement of desired outcomes for specific action, without dictating or constraining the means of achieving those outcomes.

Mindset: Hostile Predatory Environment

Doctrine: Functional Perseverance

Pending Primer

Constituency



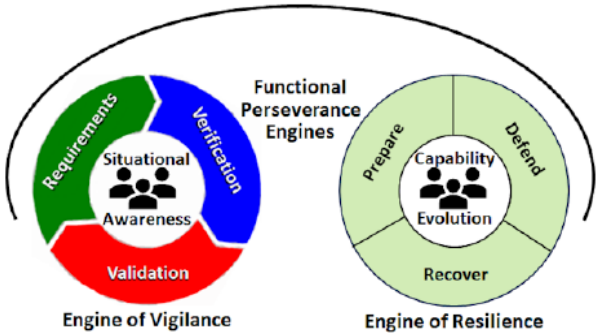
The figure highlights constituents with needs and loss concerns, aiding systems engineers in exploring, developing, and appreciating security requirements at a personal constituent level.

The constituent groups profiled are representative, not exhaustive. The needs and loss concerns listed in the table are likewise representative, not exhaustive.

The displayed profiles can sensitize requirements elicitation to the human factors. Some of the loss concerns shown, like reputation, may not be articulated. Other losses not shown are likely to be articulated with appropriate probing.

Constituents	Needs	Loss Concerns
Users	Easy/seamless security; knowledge of role & response options; …	Availability; predictable trustworthy behavior; …
Contract Customers	Short-lived adverse behavior; cost effective verification/certification; …	Value delivery; mission success; organizational reputation; …
COTS Customers	Trustworthy operation; convenient to keep secure; …	Dependability; functionality; …
Program/Product Managers	Satisfied owners/users; SE security champion; …	Acquisition satisfaction; budget and schedule performance; …
Project Managers	Comfort with security mission; knowledge of personal role; …	Personal reputation; costly delays, …
Developers	Knowledge; productivity; design requirements; …	Personal and product reputation; rework; …
Security Engineers	Early collaboration with systems engineering; meaningful requirements; …	Professional respect; ability to influence system perseverance; …
Incident Responders	Situational awareness; fallback capability; recovery/restoration capability; containment capability; …	Personal reputation; operational ownership; system functionality; behavior visibility; …
Systems Engineers	Knowledge of needs and loss concerns; perseverance/performance balance; …	Personal and product reputation; system functionality; …

Perseverance Engineering



Vigilance is sustained by situational awareness, and manifests as three systems engineering activities that drive capability evolution.

Requirements

Needs oriented, loss-driven, capability-based security requirements are naturally suited to the identification of capabilities needed by the engine of resilience. Identifying intolerable loss requires neither knowledge of vulnerabilities that can cause the loss, nor knowledge of how to protect against the loss—common sense is required, not security expertise.

Verification

A fundamental systems engineering skill—close-the-loop due diligence that all required capabilities are in fact present. Test system perseverance before Predators do.

Validation

In a static sense this is a quality issue—are the requirements sufficiently comprehensive? In a dynamic sense this is a time-based issue—has the situation changed?

Situational Awareness

Predators study targets continuously for vulnerabilities, and innovate continuously as old methods become ineffective. Previous validation of capability-needs deteriorates, and relies on awareness to trigger a new requirements cycle. Situational awareness as a functional activity should remain an active part of the system throughout its life cycle.

Resilience is sustained by capability evolution and manifests across three time frames: before, during, and after confrontation events.

Prepare

Preparation includes development and employment of technology (e.g. standards, COTS mechanisms, detectors, encryption algorithms), and leverages security education, coaching, training, and response exercises.

Defend

Given the predatory nature of the system environment, incident response is inevitable and the active part of system perseverance. Facilitating incident response and responders is preferable to paying ransom or killing a rogue system.

Recover

Preparation and defense, no matter how good, cannot preclude the possibility of functional impairment. Recovery capabilities can run the gamut from slow repair to instant replacement and can lean on emerging understandings from systems resilience engineering.

Capability Evolution

Spurred by predatory attack evolution, a system's security mechanisms evolve, or the system ceases to be viable. Emerging understandings about the linkage between innovation and agile systems can inform architectures that enable evolutionary leadership. Capability evolution as a functional activity should remain an active part of the system throughout its life cycle.

Pending Primer

Systems Engineers in the Security Equation

The Perseverance Point of View

- … is not about security (a means), it is about staying alive (an outcome).
- … is not about being everyone's job (making it no one's job), it is about being a team sport (with a role for every player).
- … is not about security engineers (protectors and defenders), it is about systems engineers (setting team objectives, weighing security tradeoffs, coaching team play).
- … is not about the system (a constructed object), it is about the constituency that serves and is served by the system (an organic group of dependents).

What's New

Systems engineering has always addressed the need for system endurance. This is not a new concern. However, what is new includes:

- Predatory intelligence: Today endurance must contend with goal-directed intelligent interventions increasingly armed with AI capabilities.
- Broadened scope of systems-as-targets: Any system whose functional interruption could cause harm or disadvantage could be a target.
- Accessible system controls: Software-based electronic control systems are network accessible, providing access to predators through wired or over-the-air connections.

What's Newish?

- Perseverance requirements engineering: needs-oriented, loss-driven, capability-based.
- Systemic situational awareness.
- Systemic capability evolution.
- Coaching constituents in their security roles.
- Emphasis on Resilience.

What's Not?

- Systems engineering
- Requirements engineering
- Verification and validation
- Team coaching

Coaching a Team

To say that security is everybody's job aptly expresses that anyone unconscious of, ignoring, or countering common sense security practice can be the leverage point of a predatory attack. More useful, however, is to view security as a team sport. In a team sport everyone has a known and relevant role to play, and coaches that help them understand and excel in that role.

Systems engineers can use requirements and other SE activities to guide the engineering team, especially development and security engineers. Shared documents like the Concept of Operations, the Operations Concept, and Systems Engineering Management Plan can be used to guide others in their roles.

References

Scheuer, A. & Wilson, B. (2024). Guide to Security Needs and Requirements. International Council on Systems Engineering. 1-August.

Dove, R., Humes, M., Leach, G., Massey, R., Ourada, G., Papke, B., Scheuer, A., Span, M., Sudmeier, D., Thomas, L., Williams, A., Wilson, B., & Winstead, M. (2025). Systems Engineering with Attitude. Proceedings International Symposium. International Council on Systems Engineering. Ottawa, CA, July 26-31.

Authors

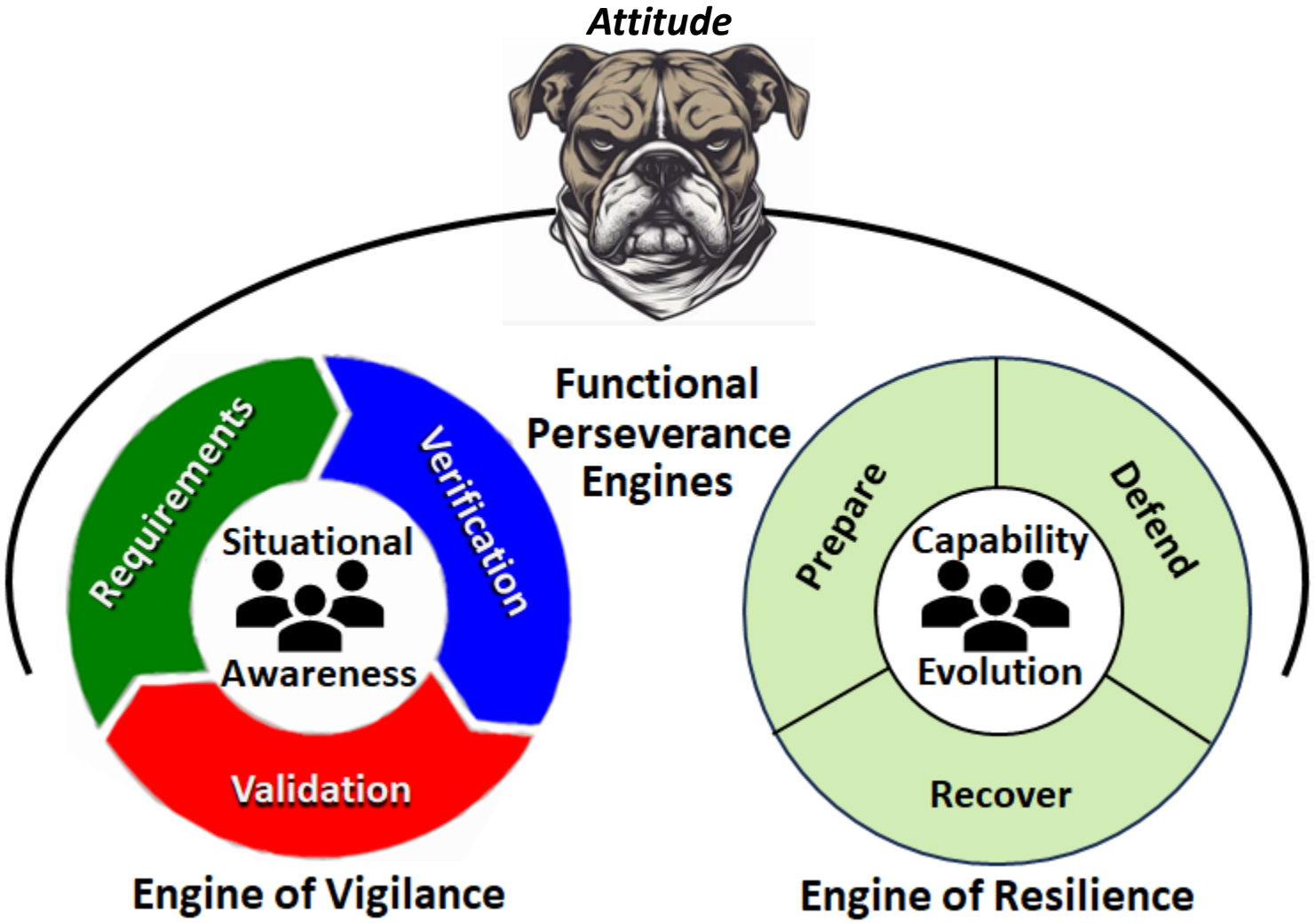
Dove, R., Humes, M., Leach, G., Massey, R., Ourada, G., Papke, B., Scheuer, A., Span, M., Sudmeier, D., Thomas, L., Williams, A., Wilson, B., & Winstead, M.

Copyright

Systems with *Attitude*

(that's the dog's name)

Comments? Questions?

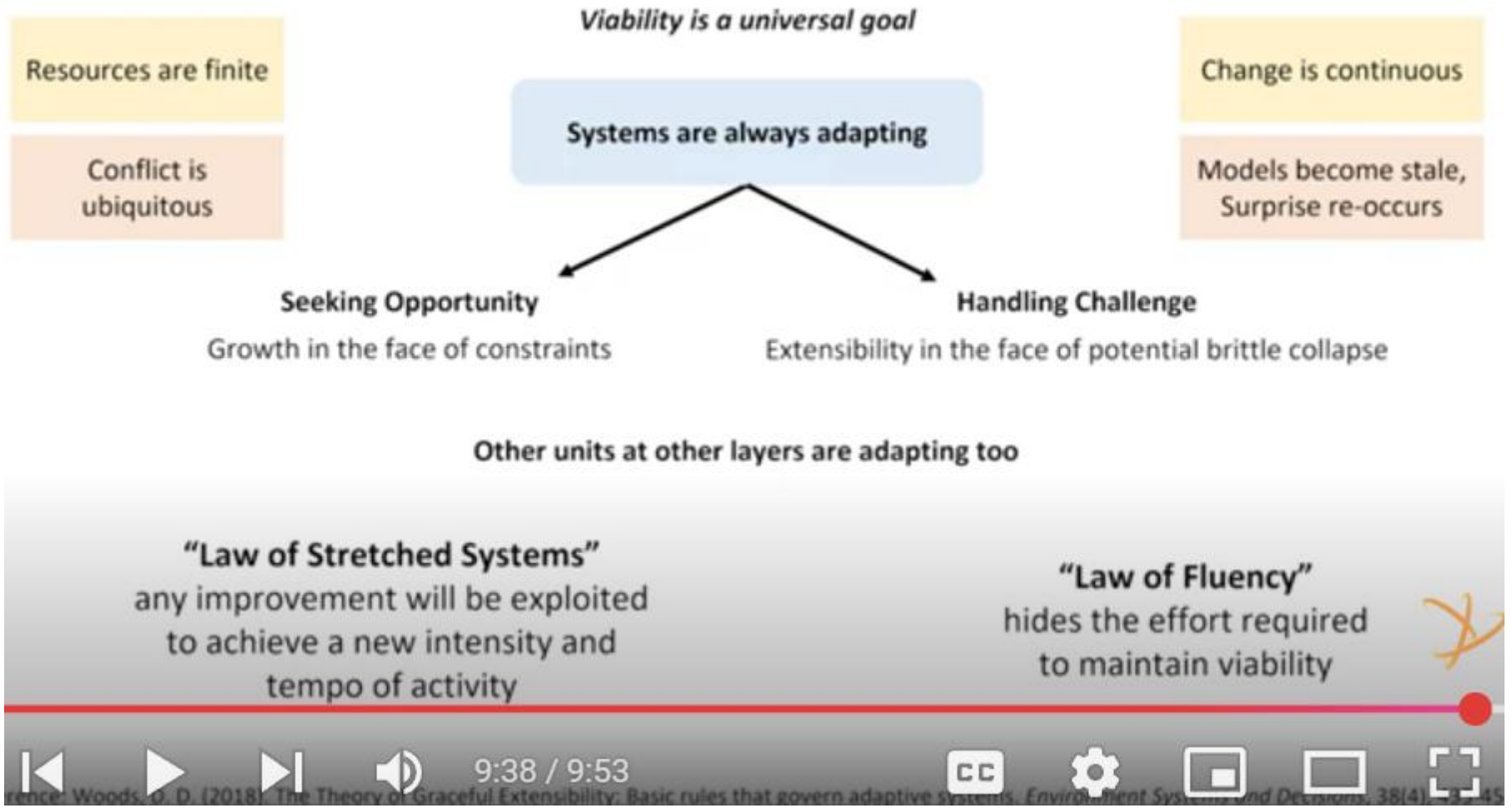


Some Next Steps

Resilience Engineering 101: Part 1 = It's all about viability

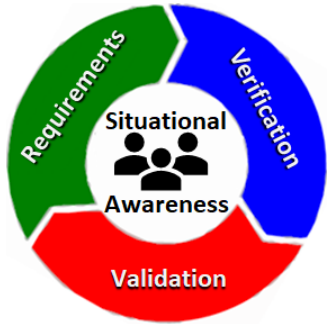
https://www.youtube.com/watch?v=Y20ssNkxuds&list=PLvlZBj1NU_in4TgQ2HFoztPMETMNRfFPl

David Woods



Woods may have the Engine of Resilience in perspective.

Woods (2018). The theory of graceful extensibility: basic rules that govern adaptive systems, www.researchgate.net/publication/327427067



Engine of Vigilance

Boyd's OODA Loop

https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2683228/Boyds%20OODA%20Loop%20Necesse%20vol%205%20nr%201.pdf

Chet Richards, 2020 Paper

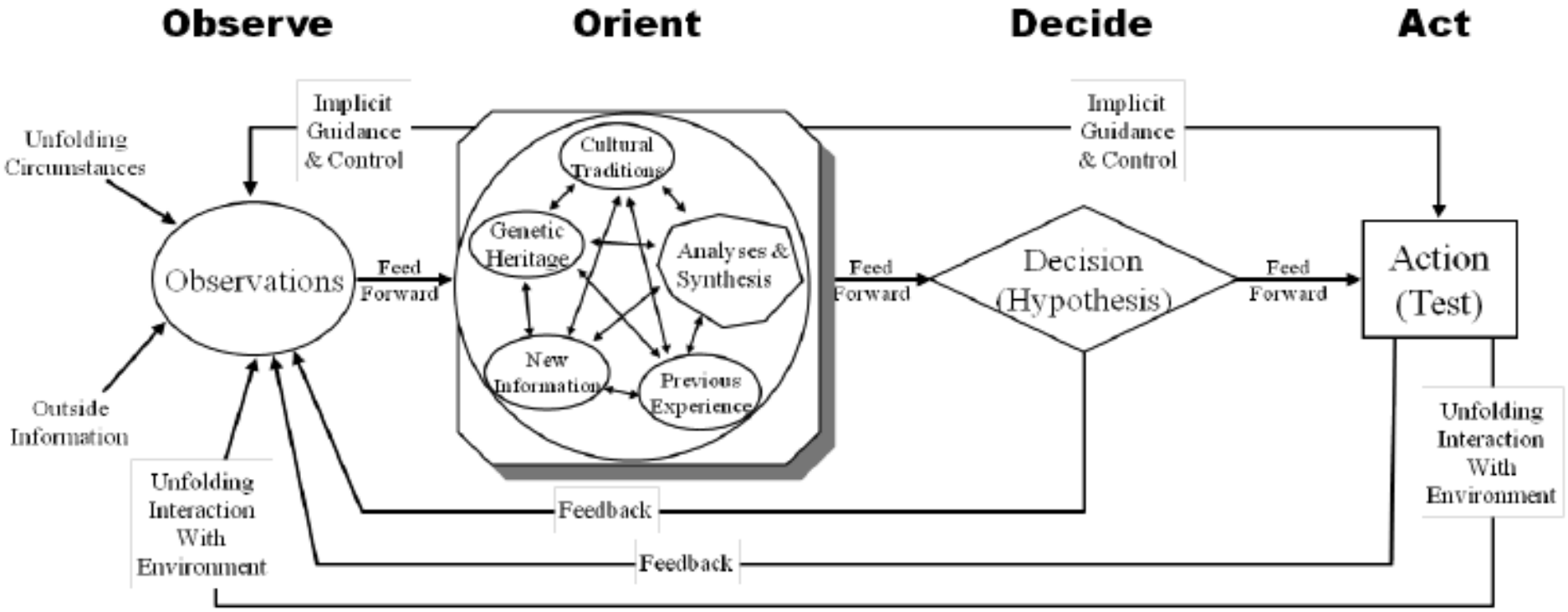
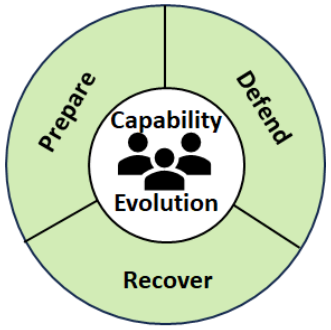


Figure 2. The only OODA "loop" that Boyd actually drew.

May provide workable ideas for getting inside the adversary's OODA loop.
OODA may have the Engine of Vigilance in perspective.



Engine of Resilience