2021 Virtual Systems & Mission Engineering Conferenc

Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundation Concepts

December 7, 2021

Presentation: Rick Dove

Authors: Rick Dove, Keith Willett, Tom McDermott, Holy Dunlap, Cory Ocker, Delia MacNamara

Approved for Public Release

The Future of Systems Engineering (FuSE)

A multi-organization INCOSE-led initiative
pursuing the systems engineering Vision.

To accomplish this the FuSE initiative encompasses a number of topic areas with active projects to shape the future of systems engineering.

INCOSE's Systems Security Engineering working group is addressing the FuSE System Security topic area and has identified a roadmap of eleven foundational concepts appropriate for near-term attention.

A brief overview of the eleven concepts follows.

INCOSE FuSE

Future of Systems Engineering

FuSE Collaborative Community

Collaborating Organizations
INCOSE
International Council on Systems Engineering
IEEE
Advancing Technology for Humanity
ITEA
APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY
ISSS
NDIA
National Defense Industrial Association
SAE
INTERNATIONAL
Software Engineering Institute
Carnegie Mellon University
SYSTEMS ENGINEERING
Research Center
MORS
DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

FuSE Road Map (~January 2020)

Theoretical Foundations
AI&SE
Complexity
Agility
Computing Advances
System Security

INCOSE Vision 2025 on Security

The principle purpose of FuSE is to realize the vision for the future of systems engineering.

"Systems engineering routinely incorporates requirements to enhance systems and information security and resiliency to cyber threats early and is able to verify the cyber defense capabilities over the full system life cycle, based on an increasing body of strategies, tools and methods. Cyber security is a fundamental system attribute that systems engineers understand and incorporate into designs."

Vision 2035 will be published in January 2022

FuSE System Security

**2020 Activity: Identify foundation gaps appropriate to fill in the near term future,
ie, a roadmap of the next part of the security journey,
not a road atlas of every point of interest.**

**2020 was about concept identification, not a handbook of practice mastery,
i.e., we need new starting points to fill some capability gaps.**

What is impeding the practice of system security that could be rectified now?

FuSE System Security Charter (2020)

INCOSE FuSE Future of Systems Engineering

Systems Security in the Future of Systems Engineering

(a FuSE initiative project)

What will good look like when we use FuSE to deliver systems?

1. All stakeholders share common security vision and respect.
2. Security is embedded in systems.
3. Security agility is in practice.
4. Systems are built for trust.
5. System and component behavior is monitored for anomalous operation.
6. System components are self protective.

Objectives

What will good look like in 2023-2025?

1. Security responsibility and expertise is integrated in the SE-team.
2. Security is viewed as a functional requirement.
3. Security agility will have some effective working patterns in practice as an early base line.
4. Strategies for shared security vision and respect in early practice.

What will good look like by end of 2020?

1. Multi-organization collaboration is active.
2. Initial foundation concepts for FuSE Security identified.
3. Projects to develop and publish some of the foundation concepts are active.

Team:

DoD –	Keith Willett
INCOSE –	Rick Dove (Project Lead)
ISSS –	Delia Pembrey MacNamara
NDIA –	Holly Dunlap, Corey Ocker
SERC –	Tom McDermott

What is stopping us from doing this now?

1. SE relates to SSE as an independent specialty practice.
2. Security is viewed as a non-functional cost and ROI value is difficult to verify.
3. Security standards compliance is considered sufficient.
4. Actionable research is in early stages.
5. Contracts and projects detail features and requirements up front rather than desired capabilities that allow innovative solutions.

2020 Action Plan

1. IS20 initial foundation papers:
   - Techno-Social Contracts for Security Orchestration.
     www.parshift.com/s/200718IS20-FuSETechnoSocialContracts.pdf
   - Contextually Aware Agile Security.
     www.parshift.com/s/200718IS20-FuSEAgileSecurity.pdf
   - Toward Architecting the Future of System Security.
     https://onlinelibrary.wiley.com/doi/abs/10.1002/j.2334-5837.2020.00717.x
2. Mid 2020: Periodic web workshops in process identifying additional foundation areas.
3. Ongoing: Recruit foundation developers.
4. Late 2020: Additional foundation papers in process.

Objectives

1. All stakeholders share common security vision and respect. Many types of stakeholders are involved in the development, usage, and sustainment of a system designed for purpose. That purpose can be compromised by the weakest security link among the stakeholders, which may stem from insufficient security respect or unresolved priority conflicts.
2. Security is embedded in systems. Rather than two engineering groups designing two systems, one intended to protect the other, systems engineering specifies and designs a single system with security embedded in the system and its components.
3. Security agility is in practice. The attack community is agile in method innovation and target selection. System security needs a response capability equally agile, architected for proactive composability and reactive resilience.
4. Systems are built for trust. Trust is accepted dependence on the system, by both stakeholders and other systems. The reasons for trusting a system need to be built in and evident to all stakeholders.
5. System and component behaviors are monitored for anomalous operation. Adversaries innovate new attack methods to evade known-pattern detection screening. System and component behavior outside of normal expectations is a method-agnostic telltale.
6. System components are self protective. System componentry is augmented, upgraded, and replaced over time by methods and personnel that cannot be unequivocally trusted.

TRL Framework (Technology Readiness Level)

Level	Definition	DoD DAG Description
1	Basic principles observed and reported	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.
2	Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3	Analytical and experimental critical function and/or characteristic proof of concept.	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4	Component and/or breadboard validation in laboratory environment.	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.
5	Technology validated in relevant environment	
6	Technology demonstrated in relevant environment	
7	System prototype demonstration in operational environment	
8	System complete and qualified	
9	Actual system proven in operational environment	

2020 FuSE System Security project focused on identifying concepts to start work on in 2021.

Foundation Concept – Criteria

Concept can provide new and useful value to the state of practice.

Concept has relevance to systems engineering considerations.

Concept value proposition can be articulated in SE terms.

Concept can be supported by notional examples.

Concept doesn’t yet have sufficient published exposure for broad SE consideration.

Concept could (or might) be prototyped now.

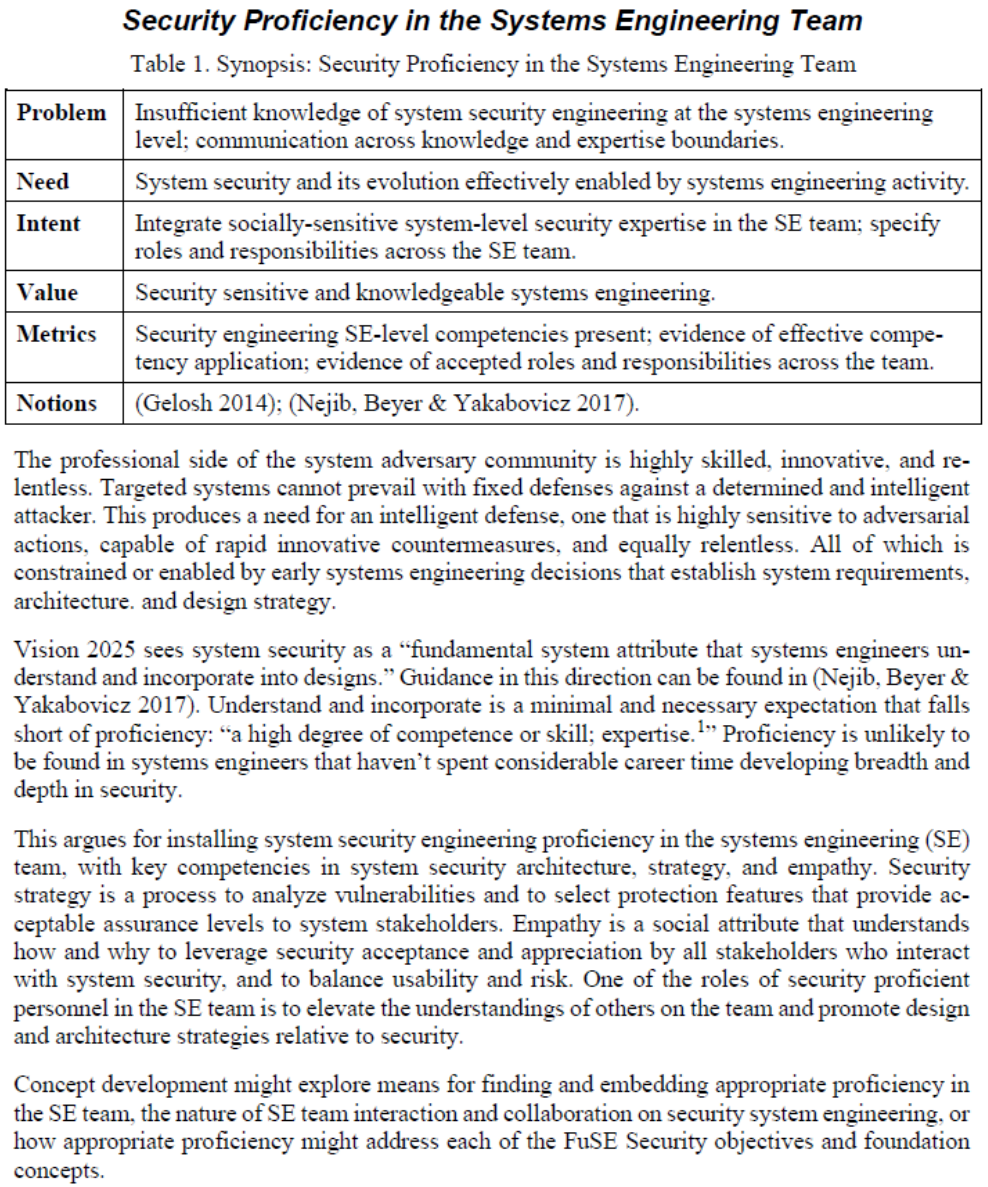
Concept is principally about why and desired outcome (strategic intent),
rather than what and how (prescriptive tactics), though examples of how lend credence.

Purpose of foundation concept papers is to inspire and instigate pursuit in the systems engineering security communities.

Development of concept papers is encouraged and open to anyone, individually or in collaboration.

TRL 1, 2, 3, 4

Eleven Concept Descriptions – One Per Page



Security Proficiency in the Systems Engineering Team

Table 1. Synopsis: Security Proficiency in the Systems Engineering Team

Problem	Insufficient knowledge of system security engineering at the systems engineering level; communication across knowledge and expertise boundaries.
Need	System security and its evolution effectively enabled by systems engineering activity.
Intent	Integrate socially-sensitive system-level security expertise in the SE team; specify roles and responsibilities across the SE team.
Value	Security sensitive and knowledgeable systems engineering.
Metrics	Security engineering SE-level competencies present; evidence of effective competency application; evidence of accepted roles and responsibilities across the team.
Notions	(Gelosh 2014); (Nejib, Beyer & Yakabovicz 2017).

The professional side of the system adversary community is highly skilled, innovative, and relentless. Targeted systems cannot prevail with fixed defenses against a determined and intelligent attacker. This produces a need for an intelligent defense, one that is highly sensitive to adversarial actions, capable of rapid innovative countermeasures, and equally relentless. All of which is constrained or enabled by early systems engineering decisions that establish system requirements, architecture, and design strategy.

Vision 2025 sees system security as a “fundamental system attribute that systems engineers understand and incorporate into designs.” Guidance in this direction can be found in (Nejib, Beyer & Yakabovicz 2017). Understand and incorporate is a minimal and necessary expectation that falls short of proficiency: “a high degree of competence or skill; expertise.[1]” Proficiency is unlikely to be found in systems engineers that haven’t spent considerable career time developing breadth and depth in security.

This argues for installing system security engineering proficiency in the systems engineering (SE) team, with key competencies in system security architecture, strategy, and empathy. Security strategy is a process to analyze vulnerabilities and to select protection features that provide acceptable assurance levels to system stakeholders. Empathy is a social attribute that understands how and why to leverage security acceptance and appreciation by all stakeholders who interact with system security, and to balance usability and risk. One of the roles of security proficient personnel in the SE team is to elevate the understandings of others on the team and promote design and architecture strategies relative to security.

Concept development might explore means for finding and embedding appropriate proficiency in the SE team, the nature of SE team interaction and collaboration on security system engineering, or how appropriate proficiency might address each of the FuSE Security objectives and foundation concepts.

Descriptions focus on strategic intent, leaving ample room for various approaches.

The metrics row suggests general methods for measuring concept-employment success.

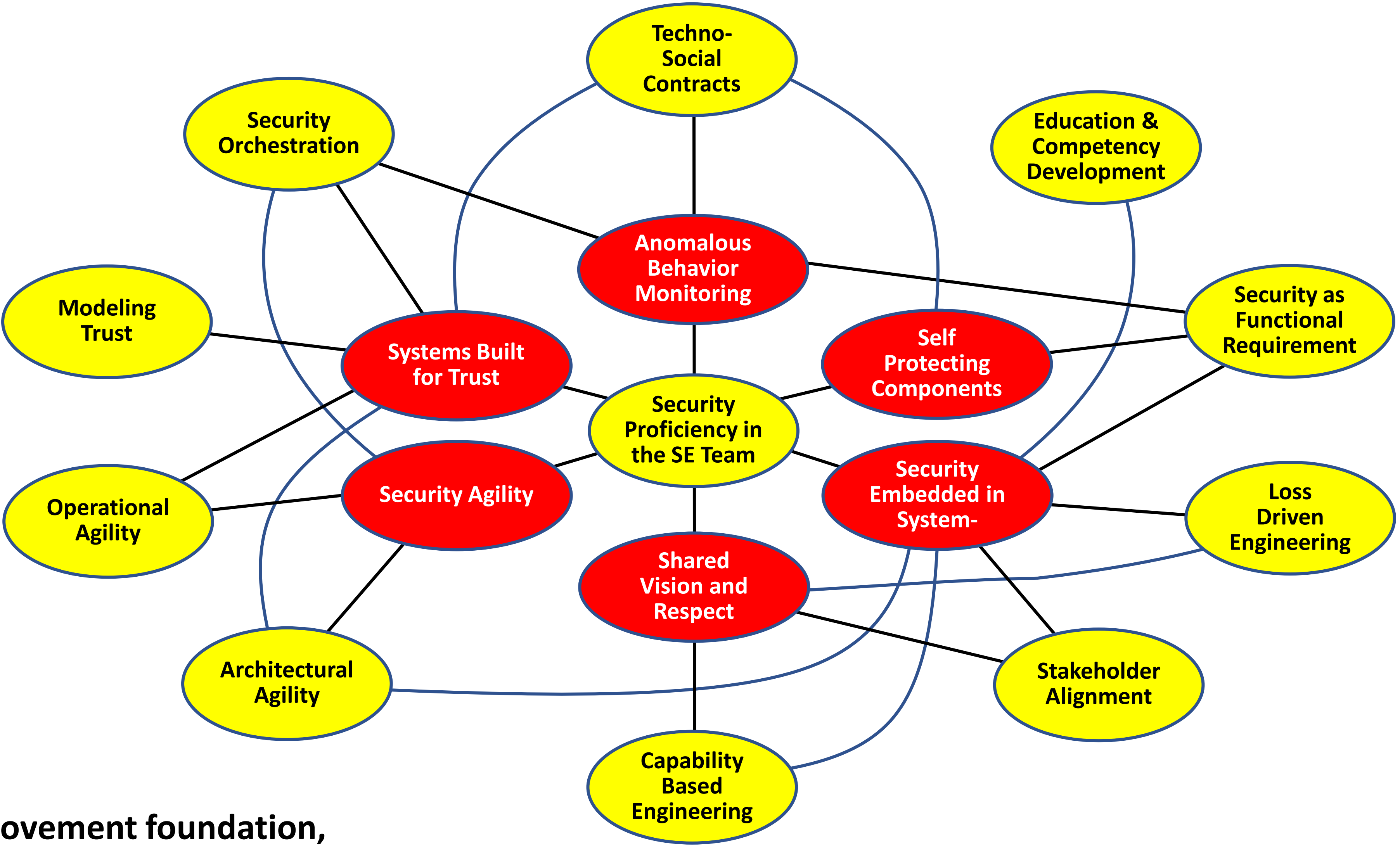
The notions row provides relevant ideas for inspiring thought without intending to constrain a solution path.

www.parshift.com/s/210717IS21-FuseSecurityRoadmap.pdf

Concept Title	General Problem to Address	General Needs to Fill	General Barriers to Overcome
1. Security Proficiency in the SE Team	Insufficient knowledge of system security engineering at the systems engineering level; communication across knowledge and expertise boundaries.	System security and its evolution effectively enabled by systems engineering activity.	Disrespect between SE and Sec people; perception of security as non-functional requirement; finding high level security expertise (architecture/strategy/empathy).
2. Education and Competency Development	Security education is not well integrated with engineering education, creating a skills gap.	Education at all levels focused on security of cyber-physical systems (CPS).	Perception of insufficient scientific/technical rigor for inclusion in engineering programs; engineering faculty security knowledge gap.
3. **Stakeholder Alignment**	Misalignment of security vision among stakeholders. Inconsistent appreciation for security among stakeholders.	Common security vision and knowledge among all stakeholders.	Stakeholder willingness to engage in collaborative convergence.
4. **Loss-Driven Engineering**	Traditional vulnerability assessments and risk/consequence models for security, safety, and related ‘ilities occur too late in the SE process.	Standard metrics and abstractions relevant to all system lifecycle phases.	Cross domain vocabulary/taxonomy differences; insufficient respect for potential leverage; solution- rather than problem-dominant security thinking.
5. **Architectural Agility**	Enabling effective response to Innovative threats and attacks.	Readily composable and re-composable security with feature variants.	Comfort with and acceptance of a dynamic security profile.
6. **Operational Agility**	Timeliness of detection, response, and recovery.	Ability for cyber-relevant response to attack and potential threat; resilience in security system.	Comfort with and acceptance of a dynamic response and recovery capability.
7. **Capability-Based Security Engineering**	Security strategies based on available solutions rather than desired results.	Top-down approach to security starting with desired results/value.	Difference between capability and features; solution-dominant thinking; trust that the outcome will be satisfactory.
8. **Security as a Functional Requirement**	As a non-functional requirement, systems security does not get prime SE attention.	Systems engineering responsibility for the security of systems.	Cultural inertia that prioritizes system purpose over viability.
9. **Modeling Trust**	Systems Security has moved away from traditional focus on trust to a more singular focus on risk.	Reinvigorate formal modeling of system trust as a core aspect of system security engineering; address issues of scale with model-based tools and automation.	Entrenched risk-based practices and education; simplicity of communicating and comparing risk metrics; perception of security as a non-functional requirement.
10.Security Orchestration	Disparate security solutions operate independently with little to no coordination.	Tightly coupled coordinated system defense in cyber-relevant time.	Independent stovepipe solution tools; multiple disparate stakeholders; hesitation to explore interdependencies
11.Techno-Social Contracts	Insufficient detection capability for innovative attack methods [with dedicated purpose security components].	Augmented detection & mitigation of known and unknown attacks [with components collaborating for mutual protection].	Trust in the security of the approach; trust in the emergent result.

FuSE System Security

Synergy Linkage Between 11 Foundation Concepts and 6 Objectives



Techno-Social Contracts
Security Orchestration
Education & Competency Development
Anomalous Behavior Monitoring
Modeling Trust
Security as Functional Requirement
Self Protecting Components
Systems Built for Trust
Security Proficiency in the SE Team
Security Embedded in System-
Security Agility
Operational Agility
Loss Driven Engineering
Shared Vision and Respect
Architectural Agility
Stakeholder Alignment
Capability Based Engineering

A near-term improvement foundation, not a comprehensive strategy web.

FuSE System Security Project – 2022+

Goals for 2022

1. Multi-organization collaboration is active.
2. All foundation concepts have publishable development
3. Foundation concept practice development is in early-stage process.

Action Plan 2022+

1. Late Jan: Review article drafts for June 2022 INSIGHT Magazine on all FuSE Security concepts.
2. Instigate & inspire foundation concept development.
3. Find and publish in-practice case examples.
4. Conduct 2-Hr. virtual workshops on individual concepts (Architectural Agility might be mid-Jan)
5. Plan transition of concepts to practice.
6. Evolve roadmap as appropriate.

**If you are interested in active participation,
contact rick.dove@parshift.com**

www.parshift.com/s/210717IS21-FuseSecurityRoadmap.pdf