2022 Systems & Mission Engineering Conference

Capability-Based Security Engineering for Strategy Formulation and Stakeholder Alignment

November 3, 2022

Presentation: Rick Dove

Collaborators: Rick Dove, Holly Dunlap, Matthew Hause, Aleksandra Scalco, Garry Stoneburner, Keith Willett, Adam Williams, Beth Wilson, Mark Winstead

rick.dove@parshift.com, attributed copies permitted

Abstract

The Future of Systems Engineering (FuSE) is an INCOSE-led multiorganizational collaborative initiative pursuing INCOSE's *Vision 2035* across a number of topic areas. One of those topic areas is concerned with system security.

INCOSE's System Security Engineering working group, in collaboration with NDIA's System Security Engineering group, developed and then published in mid 2021 a near-term roadmap of eleven concepts and six objectives.

Subsequent work has been focused on advancing the understandings of those concepts sufficient to facilitate transition to operational practice.

Collaborative team work in early 2022 identified one of those eleven concepts, Capability-Based Security Engineering (CBSE), as having high value and strong synergy with virtually all of the other concepts. CBSE at core is about needs oriented requirements engineering – expressing requirements as strategic needs and desired outcome values rather than as tactical configuration and employment of readily available solutions and knowledge.

A project emerged to design a systems engineering process that channels thinking and communication of security needs as desired outcomes rather than as prescribed solutions. Expression and understanding of security requirements as needs and values offers a path for coherent stakeholder alignment, innovative solution development, and understandable strategy formulation.

This presentation will cover the considerations and status of process design, with an emphasis on means to gain traction.


SYSTEMS ENGINEERING
VISION 2035
ENGINEERING SOLUTIONS FOR A BETTER WORLD
Cyber-security
will be as foundational a perspective
in systems design
as system performance and safety
are today (p.37)
INCOSE
Vision35

Security is a Mission – Not a System

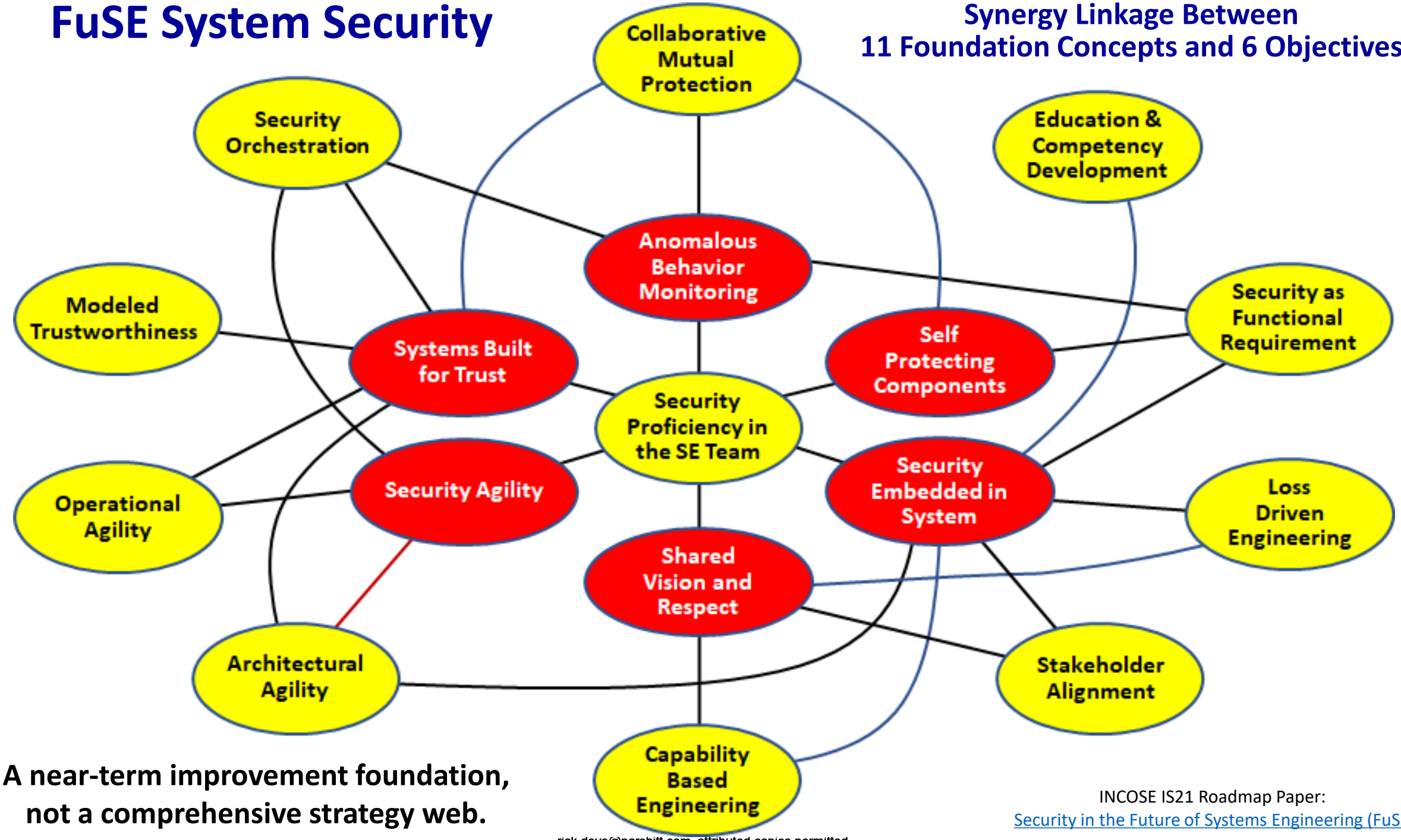
Stakeholders and technology are there to support the mission

24/7 always on:

- **situational awareness**
- **protection**
- **incident response**
- **recovery**
- **improvement**
- **evolution**

FuSE System Security

Synergy Linkage Between 11 Foundation Concepts and 6 Objectives



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

INCOSE IS21 Roadmap Paper:
Security in the Future of Systems Engineering (FuSE)

Capability Based System Security Engineering

Problem	**Security often starts with available solutions rather than desired results.**
Need	**Top-down approach to security starting with desired results/value.**
Barriers	**Difference between capability and features; solution-dominant thinking; trust that the outcome will be satisfactory; "just tell me what to do."**

A capability is an expression of a desired result agnostic of a solution that produces that result. It permits and encourages innovation.

Capability Based Engineering variations:

- **Needs Oriented Requirements Engineering**
- **Goal Oriented Requirements Engineering (GORE)**
- **Security Quality Requirements Engineering (SQUARE)**

Capability needs emerge as centrally most important:

- **They identify the foundation of a security strategy fit for context.**
- **They are intelligible to all stakeholders, a platform for alignment.**

Stakeholder Alignment

Problem	**Misalignment of security vision among stakeholders.** **Inconsistent appreciation for security among stakeholders.**
Need	**Common security vision and knowledge among all stakeholders.**
Barrier	**Stakeholder willingness to engage in collaborative convergence.**

Stakeholders of interest are not "who should be listened to;"
rather "who can affect the outcome."

We want stakeholders to come along, not go along.

We want stakeholders to be engaged in the mission.

We want an aligned sense of need, awareness, importance, attention, respect.

Well-defined capability needs are a key output from this alignment.

Security Proficiency in the SE 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.**
Barriers	**Disrespect between SE and Sec people; perception of security as non-functional requirement; finding high level security expertise.**

Proficiency exercises high-level competencies in system security thinking, architecture, strategy, and empathy.

Stakeholder alignment is the "minimum viable product" demonstrating security proficiency in the SE team.

Loss-Driven Engineering

Problem	**Traditional vulnerability assessments and risk/consequence models for security occur too late in the SE process.**
Need	**Standard metrics and abstractions relevant to all system lifecycle phases.**
Barrier	**Insufficient respect for potential leverage; solution- rather than problem-dominant security thinking.**

"There is a need to emphasize protection against the effects of loss … it is prudent to ensure that there is focus on the effect to be controlled rather than on the cause when protecting against loss." **(NIST SP 800-160 volume 1 revision 1)**

Protection from losses are understandable to a broad base of stakeholders as needs.

Modeling Trustworthiness

Problem Systems Security has moved away from its traditional focus on trust to a more singular focus on risk.

Need Reinvigorate formal modeling of system trust as an evidentiary core aspect of system security engineering.

Barrier Entrenched risk-based practices and education; simplicity of communicating and comparing risk metrics; perception of security as a non-functional requirement.

Security functions and assurance processes became separated in the early 2000s.

Since then the concepts of risk and assurance have dominated the community.

The community needs a return to "Security as a functional requirement" supported by formal security models that support system engineering decisions and V&V activities.

Evidence meriting trustworthiness by stakeholders can be modeled to show functional capabilities linked to needs.

Security as a Functional Requirement

Problem As a non-functional requirement, systems security does not get prime system engineering attention.
Need Systems engineering responsibility for the security of systems.
Barrier Cultural inertia that prioritizes system purpose over system viability.

System security engineering is concerned with achieving capabilities that satisfy stakeholder-defined needs.

To ensure security is designed in, these capabilities must be specified as functional requirements.

A functional requirement is a qualitative description of an activity to perform or purpose to achieve *in fulfillment of a need*.

Security Orchestration

Problem	**Disparate security solutions operate independently with little to no coordination.**
Need	**Tightly coupled coordinated system defense in cyber-relevant time.**
Barrier	**Independent stovepipe solution tools; multiple disparate stakeholders; hesitation to explore interdependencies**

Security Orchestration provides a foundation to explore and develop autonomous governance and adjudication logic for dynamic security decisions in operations, for fast, relevant, and adaptable system defense.

Orchestration invokes static solutions as standard sequences, and dynamic solutions as composition (from available assets) or dynamic development (real-time production).

A cultural twist that requires stakeholder alignment on the need for (some) autonomous mission management and alignment on the means for exploring functional and cultural compatibility.

Collaborative Mutual Protection

Problem Insufficient detection and response capability for innovative attacks with infrastructure-based security mechanisms.
Need Widely distributed detection & mitigation of known and unknown attacks.
Barrier Trust in the security of the approach; trust in the emergent result.

Mutual protection behavior among technical system components is both beneficial and possible.

Beneficial in that security collaboration, cooperation, and teaming among system elements during system operation offers novel strategy for quick detection and mitigation of innovative security threats.

Possible in that human and animal communities employ effectively demonstrated approaches, and non-organic socially cooperating system aggregations already exists in the fields of robotics, drone swarms, and Mobile Ad Hoc Networks (MANETs).

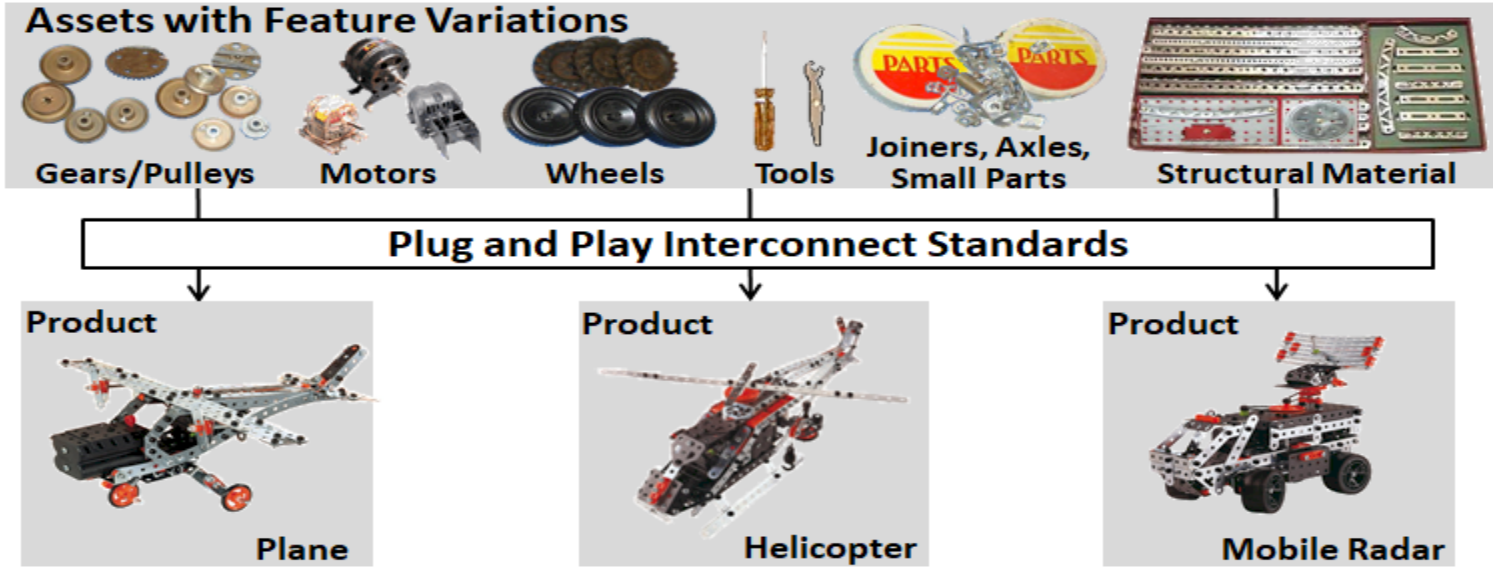
A human community concept understandable as a strategy and as a mission; but a twist on traditional security in need of stakeholder alignment for distributed interaction.

Architectural Agility

Problem Enabling effective response to Innovative threats and attacks.
Need Readily composable and re-composable security with feature variants.
Barrier Comfort with and acceptance of a dynamic security profile.

A product line security architecture with a product-family asset management strategy enables security resilience and composable innovation; and facilitates coherent security evolution.

A cultural twist that requires stakeholder alignment on the need for an agile capability and alignment on the means for exploring functional and cultural compatibility.



Operational Agility

Problem	**Timeliness of detection, response, and recovery.**
Need	**Ability for cyber-relevant response to attack and potential threat; resilience in security system.**
Barrier	**Comfort with and acceptance of a dynamic response and recovery capability.**

Operational agility provide real-time composable response options in an operational environment that can present innovative threats continuously.

Architectural agility provides coherent response options for operational agility to select and execute as appropriate to the moment.

A cultural twist that requires stakeholder alignment on the need for agile operations and alignment on the means for exploring functional and cultural compatibility.

Education and Competency Development

Problem	**Security education is not well integrated with engineering education, creating a skills gap.**
Need	**Education at all levels focused on security of cyber-physical systems (CPS).**
Barrier	**Perception of insufficient scientific/technical rigor for inclusion in engineering programs; engineering faculty security knowledge gap.**

Systems engineering is not addressing security well enough and is not addressing the specific concerns emerging in today's embedded systems and cyber physical systems.

Supply is created and sustained by demand. Educators and trainers on the supply side and acquirers and developers on the demand side can both contribute.

Security needs and strategy independent of implementation tactics can be taught and absorbed by a broad range of educators and engineers.

Holistic

more than the sum of the parts

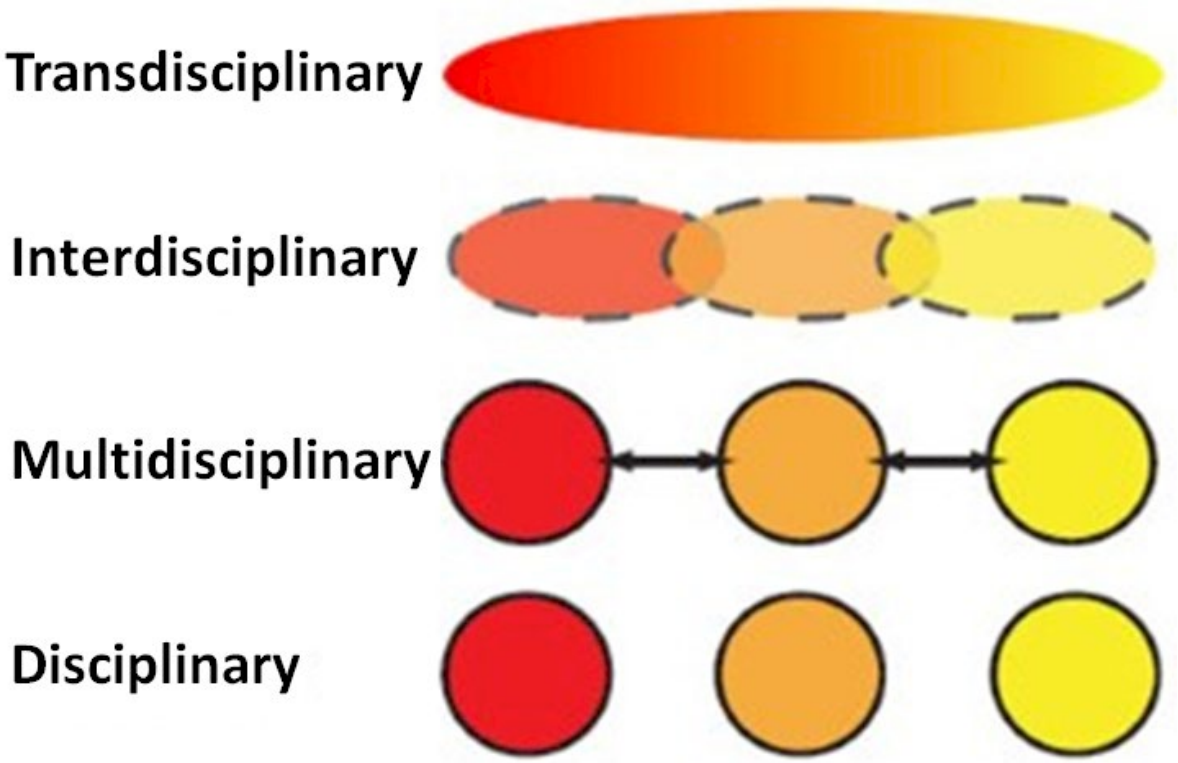
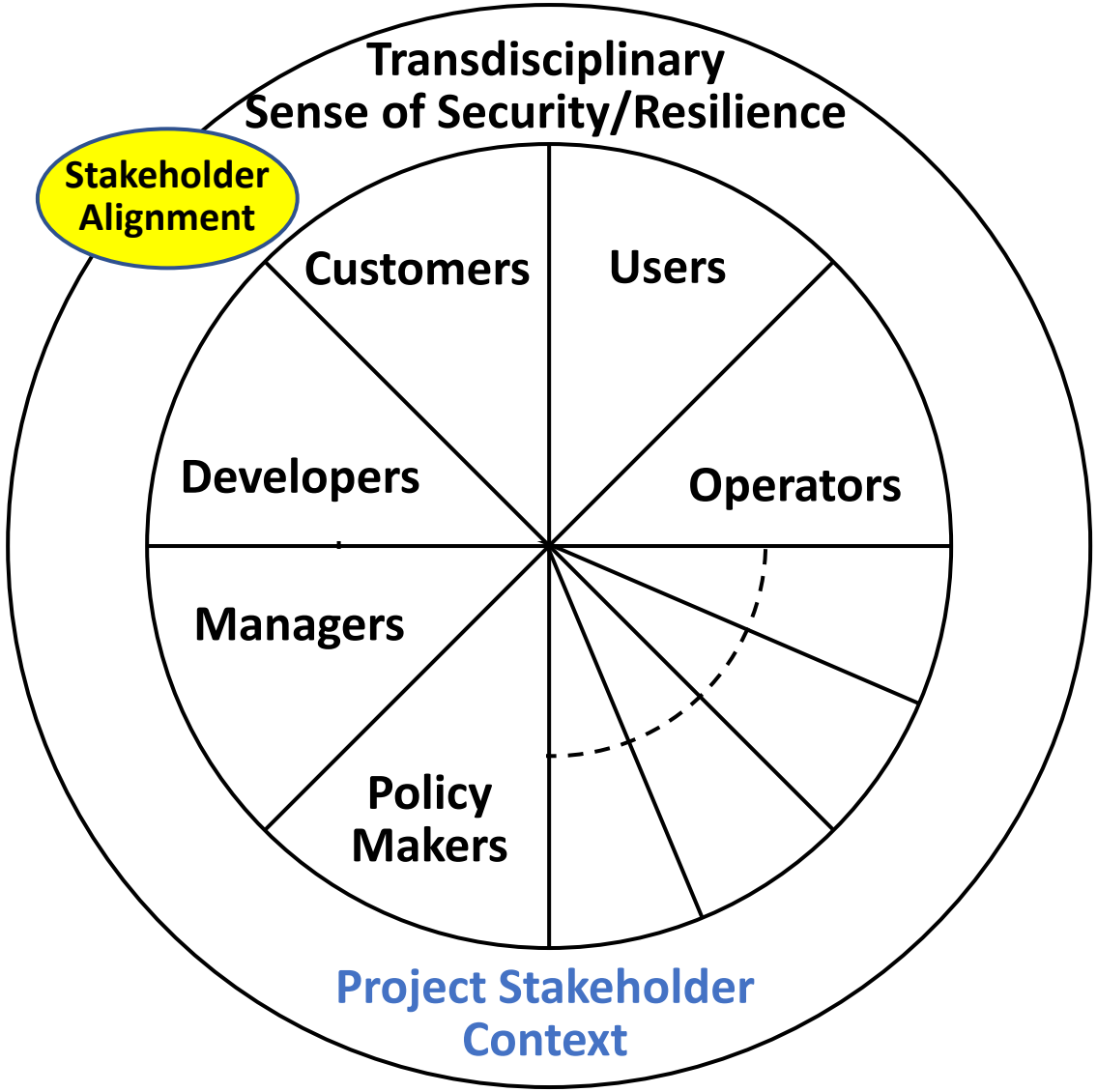


Figure Credit: https://doi.org/10.1038/nchembio0908-511
Colón, W., *et al.* Chemical biology at the US National Science Foundation.



A higher sense of common relevance.

An aligned sense of need, importance, awareness, attention, respect.

Security Quality Requirements Engineering (SQUARE)

Stakeholder alignment around goals to satisfying needs – proof of concept

Lessons Learned:

- **Every project is different, requiring tailored process flexibility.**
- **Facilitating reusable techniques, goals, and capabilities reduces cost and speeds results.**

Our interest is in the first 2 of 9 SQUARE Steps

Step 1: Agree on definitions (a technique for revealing stakeholder knowledge and misalignments)
Input – Candidate definitions from IEEE and other standards
Technique – Structured interviews, focus group
Participant –Stakeholders, requirements team
Output – Agreed-to definitions

Step 2: Identify security goals
Input – Definitions, candidate goals, business drivers, policies and procedures, examples
Technique – Facilitated work session, surveys, interviews
Participant – Stakeholders, requirements engineer
Output – Goals

SEI (N. R. Mead, E. D. Hough, T. R. Stehney II). 2005. Security Quality Requirements Engineering (SQUARE) Methodology.
SEI. 2008. SQUARE-Lite: Case Study on VADSoft Project
SEI. 2010. Security Requirements Reusability and the SQUARE Methodology

We* want to ensure and hasten this Vision.

It is Cultural.
It is a mind set.

Cornerstones:
Stakeholder Alignment and Capability Based Security Engineering.

*INCOSE Systems Security Engineering working group. Chair: dove@parshift.com

Every project has different needs, different stakeholders.

The Vision will occur as grass roots initiatives.

Security is a community affair, not a proprietary competitive advantage.

We want case studies and lessons learned.

We will help develop these if you like.

- Setting Current Context for Security in the Future of Systems Engineering
- Measuring Stakeholder Alignment to Overcome Control System Cyber Vulnerability
- Functionally Interpreting Security
- Capability Engineering vs. "Problemeering" and "Solutioneering"
  - Prioritizing Stakeholder Needs over Requirements
- Very Small Entities (VSE): Outsourcing Risk to the Supply Chain Is Placing Systems Security Engineering on a Clay Foundation, but Playing Games May Help
- Framework for Operational Resilience in Engineering and System Test (FOREST)
  Part I: Methodology Part II: Case Study
- Modeling for Trustworthiness
- Multilayered Network Models for Security: Enhancing System Security Engineering with Orchestration
- Making the Puzzle Pieces Fit - Utilizing UAF to Model a Cybersecurity SoS
- Analyzing System Security Architecture in concept phase using UAF domains
- Cyber Supply Chain Risk Management (C-SCRM) a System Security Engineering Role in the Future of Systems Engineering

References

Dove, R., K. D. Willett. 2020. Techno-Social Contracts for Security Orchestration in the Future of Systems Engineering. INCOSE IS20. Virtual. www.parshift.com/s/200718IS20-FuSETechnoSocialContracts.pdf

Dove, R., Willet, K., McDermott, T., Dunlap, H., MacNamara, D.P., and Ocker, C., 2021. Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundational Concepts. INCOSE International Symposium, Virtual: July 17-22. http://www.parshift.com/s/210717IS21-FuseSecurityRoadmap.pdf

Evans, J. July 29, 2014, What is Transdisciplinarity? Purdue Polytechnic Institute. https://polytechnic.purdue.edu/blog/what-transdisciplinarity

Maguire, L. 2020. How Many Is Too Much? Exploring Costs of Coordination During Outages. QCon London, May 11. Video and transcript at www.infoq.com/presentations/incident-command-system

Scalco, A. 2022. Measuring Stakeholder Alignment to Overcome Control System Cyber Vulnerability. INSIGHT, Vol. 25, No. 2. INCOSE. June.

SEI (N. R. Mead, E. D. Hough, T. R. Stehney II). 2005. Security Quality Requirements Engineering (SQUARE) Methodology. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2005_005_001_14594.pdf

SEI. 2008. SQUARE-Lite: Case Study on VADSoft Project. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8483

SEI. 2010. Security Requirements Reusability and the SQUARE Methodology. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15197.pdf

Tu, C.Z., Yuan, Y., Archer, N. and Connelly, C.E. 2018. "Strategic value alignment for information security management: a critical success factor analysis." Emerald Publishing Limited, Information and Computer Security, Vol. 26 No. 2, pp. 150-170. www.sci-hub.se/10.1108/ICS-06-2017-0042