33rd Annual INCOSE international symposium
hybrid event
Honolulu, HI, USA
July 15 - 20, 2023

Democratizing Systems Security

Rick Dove
Independent
dove@parshift.com

Mark Winstead
MITRE Corp.
mwinstead@mitre.org

Holy Dunlap
MITRE Corp.
hdunlap@mitre.org

Matthew Hause
SSI
MHause@systemxi.com

Dr. Aleksandra Scalco
INCOSE
aleksandra.scalco@incose.net

Dr. Keith Willett
US Dept. of Defense
kwillett@ctntechnologies.com

Dr. Adam D. Williams
Sandia National Labs
adwilli@sandia.gov

Dr. Beth Wilson
Independent
wilsondrbeth@aol.com

Abstract. As systems security joins the top concerns of systems engineering, the availability and affordability of already scarce security expertise presents a resource barrier and raises questions about the nature of competency needed in the systems engineering team. Workshops in 2022 exploring the eleven strategies outlined in the 2021 roadmap for Security in the Future of Systems Engineering revealed one strategy as centrally synergistic with all the other ten: Stakeholder Alignment. Investigating means and effects of aligning stakeholders on security requirements led to the understanding that security expressed as loss-driven needs and capabilities would be accessible to everyone, independent of how those needs and capabilities would be realized. This article makes a case for achieving stakeholder security alignment as a means to efffectualize security as a foundational perspective in system design and actualize security proficiency in the SE team.

Introduction

INCOSE's Systems Engineering Vision 2035 expects that "security will be as foundational a perspective in systems design as system performance and safety are today (INCOSE 2021, p. 37)". No argument is heard against the value of this, but how will it come to pass? Is this wishful thinking or does it lead to a feasible outcome?

In the spirit of Vision 2035's expectation, this paper is concerned with systems security in the broadest sense, where the system of interest, in whatever software, hardware and people that includes, defines the boundary of the system we wish to be secure.

In systems engineering performance and safety are front-burner objectives; a system short on either is not viable. But a system that can perform safely but not reliably isn't viable either. As stakeholders we know the systems we build or acquire are targets for attack, so we engage security-development specialists and certification procedures intended to harden and verify reliability.

But reliability is fragile and illusive when stakeholders are misaligned on security needs and have offloaded the responsibility for security outcomes.

Outcome-relevant stakeholders are those who can directly affect or be affected by system security. Virtually none of them are subject matter experts in system security – they are customers, users, and developers; they are systems engineers responsible for system coherence; and they are managers of all sorts that control decision-making and work priorities.

Though they can't speak with technical expertise, all stakeholders can elucidate, or validate when prompted, what they cannot afford to lose, and what they can tolerate as partial or temporary loss. Loss may be in system functionality, in system assets, or in assets the system can affect.

> 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.

To achieve security as a broadly embraced systems foundational perspective we need understandable and meaningful security capabilities that stakeholders can articulate, support, and relate to with personal perspective as both necessary and useful. This approach is democratization: "the action of making something accessible to everyone.[1]"

Systems security is more than a collection of technologies and specialists; it is a mission that needs an aligned team of stakeholders. Stakeholders who are misaligned compromise and degrade the objectives of those who are aligned. Misalignment has a range of manifestations:

- Ignorance – oblivious.
- Apathy – aware and doesn't care.
- Friction – aware and contentious.
- Contradiction – aware and at odds.
- Counteractive – not intentional, just myopically unaware of the outcome.
- Subversive – purposeful sabotage.

Stakeholders who are aligned appreciate the needs of others, share their needs and priorities with others, seek non-conflicting understandings of collective needs, and will revamp personal requirements that would impair the security needs of others even if they don't feel those exact needs.

Different types of stakeholders have different security perspectives. As a sampling:

- Contract acquisition wants unimpeded delivery.
- Purchase acquisition wants functional sustainment.
- Suppliers want a reputation for operational excellence.
- Program and project managers want no-surprise, incident-free smooth sailing.
- Developers want freedom from rework.
- Users want understandable needs satisfied with usable approaches.

INCOSE's recent publication of Systems Engineering Principles (Watson et al. 2022) addresses alignment values in general: "Each decision maker may have different preferences, beliefs, and

[1] democratization definition - Google Oxford Languages accessed 9-December-2022

alternatives. While each of these elements are challenging to understand, preferences are of particular interest to systems engineering as they relate to desired system goals. If different preferences are being used to make decisions on a system, then those decisions would be inconsistent with each other, meaning it is possible that given the same beliefs and alternatives decision makers may decide on different solutions. To enable consistent decision-making throughout the organization, systems engineers must elicit, represent, and communicate preferences of key stakeholders to drive to outcomes that the key stakeholder prefers."

The purpose of this paper is to make a case for achieving stakeholder security alignment as a means to efffectualize security as a foundational perspective in system design and actualize security proficiency in the SE team – a concept featured among the eleven outlined in the roadmap for Security in the Future of Systems Engineering (Dove et al. 2021). The next section of this paper will review each of the eleven roadmap concepts in relation to the Stakeholder Alignment concept, emphasizing the pervasive value this one concept has on all others. A subsequent section will explore some methods and cases in the literature for achieving alignment followed by a final section with concluding remarks.

Security in the Future of Systems Engineering

In 2022, workshops explored the eleven strategies (Figure 1) outlined in the 2021 roadmap for Security in the Future of Systems Engineering (Dove et al. 2021). In this exploration, one strategy emerged as centrally synergistic with all the other ten: stakeholder alignment. All leverage stakeholder alignment, are leveraged by stakeholder alignment, contribute value to stakeholder alignment, and/or gain value from stakeholder alignment.

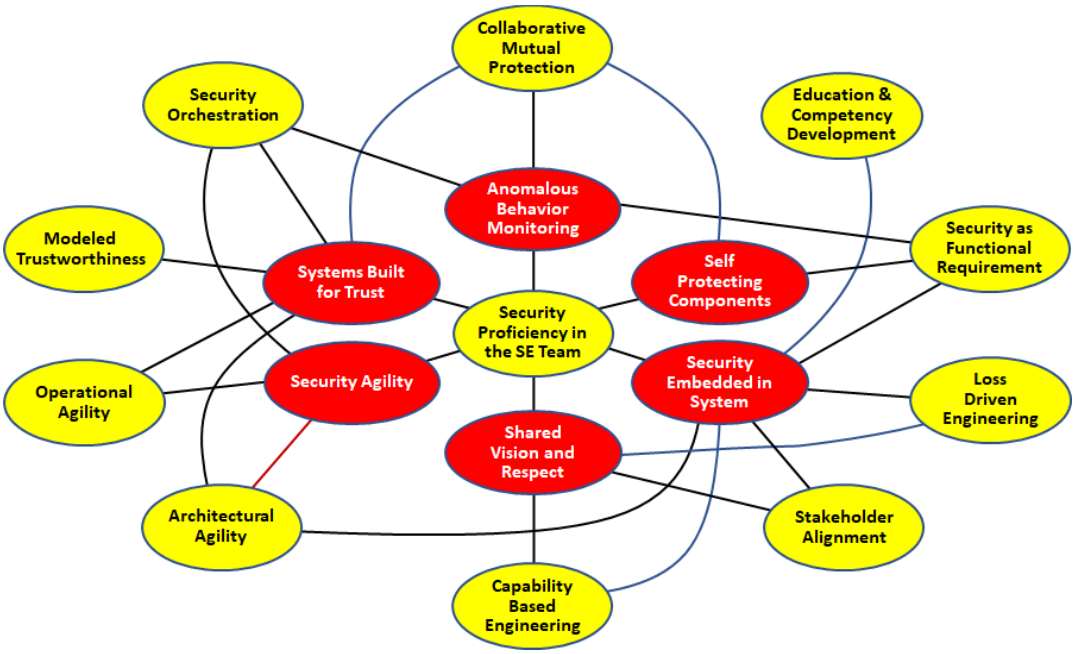

Figure 1. A strategy web depicting eleven concepts and their primary support vectors for six objectives in near-term systems security improvement (Dove et al. 2021).

We review the eleven strategies starting with stakeholder alignment, then detail the relationships of the other ten to stakeholder alignment in the rest of this section.

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;" but rather "who can affect or be affected by the outcome."

We want stakeholders to come along, not go along; to be engaged in the mission. We want an aligned sense of need, awareness, importance, attention, and respect.

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

Strategic Value Alignment for Information Security Management: A Critical Success Factor Analysis (Tu et al. 2018) suggest that security management activity "be based on business objectives, values, or needs, as opposed to being technology asset focused." Their case for alignment made from a business perspectives point of view resonates with our systems' stakeholder point of view:

> "Security is not directly linked to the mission. This often creates value conflict. For instance, managers who focus on using a company's resources for business competition may ignore security risks and optimistically think these attacks will not happen. This results from viewing information security as a burden and not wanting to spend money on it. In general, employees are expected to do good jobs in order to be rewarded. They may have value conflicts towards security and view security policy as unnecessary or interfering with productivity. From a customer perspective, the focus is to get good service conveniently. So customers may also view security measures such as complex password setting as headaches or the use of biometric identity authentication with privacy concerns. To improve information security, the key is to recognize such value conflicts and find a way to deal with them effectively. Literature has shown that the most proactive way to deal with value conflicts is to work towards value alignment. Specifically, for security-related value conflicts, it is important to create value alignment for all the parties involved in information security management."

Capability-Based Systems 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. A capability-based systems security engineering approach permits and encourages innovation.

Capability-Based Engineering variations:

- Needs Oriented Requirements Engineering (Wheatcraft et al. 2022))
- Loss Oriented Requirements Engineering (Ross, Winstead and McEvilley 2022)
- Goal Oriented Requirements Engineering (van Lamsweerde 2001)
- Security Quality Requirements Engineering (Mead, Hough and Stehney II 2005)

Capability needs emerge as centrally most important:

- They identify the foundation of a security strategy fit for the context.
- They are intelligible to all stakeholders, a platform for 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 exhibits high-level competencies in system security thinking, architecture, strategy, and user empathy.

As systems security joins the top concerns of systems engineering, the availability and affordability of already scarce security expertise presents a resource barrier and raises questions about the nature of competency needed in the systems engineering team.

The 2021 roadmap paper expected security proficiency to be a product of specialized security skills resident in the SE team. Further work in 2022, as outlined in this paper, now views relevant security proficiency as a product of systems engineering skills: stakeholder alignment and requirements engineering with a needs-oriented, loss-driven, capability-based security focus. This view has the added benefit of diffusing, as opposed to localizing, the necessary security proficiency, and can easily leverage the incorporation of deeper expertise should it become available.

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. (Ross, McEvilley and Winstead 2022)”

Protection from losses is 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 vulnerability 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 evidence-based verification and validation activities.

Evidence meriting trustworthiness by stakeholders can be modeled to show functional capabilities linked to aligned stakeholder 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 prioritizes system purpose over system viability.

Systems 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 qualitative description of an activity to perform or purpose to achieve in fulfillment of a stakeholder 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).

This cultural twist 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 offer 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 threats; resilience in security systems.
Barrier	Comfort with and acceptance of a dynamic response and recovery capability.

Operational agility provides real-time composable response options in an operating 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.

Similar to architectural agility, this is 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 the 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 needs to address security better and address the specific concerns emerging in today's embedded systems and cyber-physical systems.

Supply is created and sustained by demand. Therefore, educators and trainers on the supply side and acquirers and developers on the demand side can contribute.

Loss-driven security needs and capabilities (the core of stakeholder alignment), independent of implementation tactics, can be taught and absorbed by a broad range of educators and engineers.

Some Ideas for Aligning Stakeholders

This paper aims to explore values in achieving stakeholder security alignment. This section will review some thoughts in the literature for achieving alignment. But it is not the intent here to propose how alignment should be done. That awaits completion of further work.

We suggest that stakeholder alignment can naturally occur around a loss-driven, needs-oriented, capability-based security strategy. The loss and needs focus are relatively new, but aligning stakeholders around security capabilities rather than features is not new.

Goal-oriented requirements engineering, referred to as GORE in the literature, has a prominent literature presence starting in the 2000s. The most cited publication amongst hundreds, according to a study by (Horkoff, et al. 2017), indicates it is consistent, for our purposes, to view requirements goals as desired capabilities (van Lamsweerde, 2001); which in turn (though unsaid) are expected to fill needs. In his paper van Lamsweerde makes a case for need-fulfilling goals (capabilities) as drivers for requirements engineering:

- Goals provide a precise criterion for sufficient completeness of a requirement's specification.
- Goals provide a precise criterion for requirements pertinence.
- Goals provide the rationale for explaining requirements to stakeholders.
- Goals provide the roots for detecting conflicts among requirements.
- Goals are more stable, whereas requirements for achieving the goal are more likely to evolve.
- Goals drive the identification of requirements to support them.

What van Lamsweerde says about goal-directed requirements engineering is domain agnostic, with occasional specific excursions, e.g.: "Security goals are specialized into confidentiality, integrity and availability goals; the latter can be specialized in turn until reaching domain-specific security goals."

Subsequently, van Lamsweerde observes, "Goal identification is not necessarily an easy task. Sometimes they are explicitly stated by stakeholders or in preliminary material available to requirements engineers. Most often they are implicit so that goal elicitation has to be undertaken."

The authors of this article suggest that a loss-driven, needs-oriented focus on goal identification (capabilities) makes the task understandable and meaningful to all stakeholders.

The Software Engineering Institute (SEI) joined the fray with Security Quality Requirements Engineering (SQUARE) Methodology (Mead, Hough and Stehney 2005); a complete process with nine steps covering security requirements from high-level needs to lowest-level technical requirements. Only their first two steps are relevant to our alignment aims. Their first step offers a way to break the ice with stakeholders and reveal their levels of security understanding and interests. Their second step elicits, refines, deconflicts, and aligns high-level security goals (desired capabilities): "Initially, different stakeholders will likely have different security goals. … The security goals of the stakeholders may also conflict with one another. A security-conscious stakeholder may place high importance on strong security controls for the system, which in turn may hamper overall system performance. Decreased performance might likely be at odds with the goals of the marketing department. Step 2 in the SQUARE process serves to eliminate such conflicts and align all of the stakeholders' interests."

Mead and others at SEI have published case studies and variations on the process that can inform the development of alignment techniques. For their purposes they suggest high-level security goals should be on the order of half a dozen, with "more or less depending on the scale of the project."

The cited initial paper on the SQUARE methodology suggests: "The methodology is most effective and accurate when conducted with a team of requirements engineers with security expertise and the stakeholders of the project." SQUARE goes directly for goals (capabilities) without our

intent of loss-driven, needs-oriented qualification – which would eliminate their need for security "expertise."

A loss-driven, needs-oriented, capability-based approach is outlined very effectively in the literature, albeit without using the three-hyphens phrase directly. Nancy Levenson and others at MIT have adapted the Systems Theoretic Process Analysis (STPA) for safety requirements engineering to systems security (Young and Levenson 2014):

- "STPA-Sec is an extension to STPA to include security analysis."
- "In contrast to a tactics-based, bottom-up approach, a top-down, strategic approach starts with identifying the system losses that are unacceptable and against which the system must be protected. The result is a small and more manageable set of potential losses stated at a high-level of abstraction. These losses likely extend beyond the physical and logical system entities into the higher-level services provided by these entities."
- "Rather than starting with the tactics questions of how best to guard the network against threats, a strategic approach begins with questions about what essential services and functions must be secured against disruptions and what represents an unacceptable loss. The "whats" will be used later to reason more thoroughly about the "hows" that can lead to specific undesirable outcomes."
- "Surprisingly, while STPA is more powerful, it also appears to require fewer resources, including time. … This approach limits the intelligence burden required to perform the initial system security analysis."

All the literature references above are intended and designed to improve security requirements engineering. Our suggestion in this paper leverages security requirements engineering with a different intent: "Security will be as foundational a perspective in systems design as system performance and safety are today."

Concluding Discussion

For security to become a foundational perspective in systems design like system performance and safety, stakeholder alignment for security, like stakeholder alignment typically exists for performance and safety, is essential. Moreover, stakeholder alignment is even more crucial for security than for system performance and safety, as security is a community affair given how everything is networked and one bad apple can compromise the rest.

As captured within this paper, the series of workshops in 2022 conducted with the authors and other contributors found a strong synergy across the roadmap concepts of (Dove et al. 2021), but most especially with stakeholder alignment. The series participants concluded that a loss-driven, needs-oriented, capability-based approach could be a strong basis for achieving stakeholder alignment. But perhaps more importantly, this approach democratizes security as it gives everyone an opportunity to meaningfully participate in developing and understanding security strategy.

The arguments throughout this paper for stakeholder alignment focus on why and what as stable underpinnings, with some references provided for various hows from a literature review.

Table 1 summarizes this paper's logical/rational argument for aligning stakeholders on needs-oriented, loss-driven, capability-based security requirements.

Table 1. Summarizing values to roadmap concepts of aligning stakeholders on needs-oriented, loss-driven, capability-based security requirements.

Roadmap Concept (What)	Related Benefits (Why)
Stakeholder Alignment	A needs-oriented, loss-driven, capability-based security requirements engineering approach enables and facilitates alignment as the needs and values are understandable to non-specialists.
Capability-Based SSE	Provides systematic identification and justification of needed capabilities.
Security Proficiency in the SE Team	Provides benefits of proficiency (coherent security strategy and security as foundational perspective) without need for SE-personnel retooling or reeducation.
Loss-Driven Engineering	Provides systematic identification of unacceptable and tolerable losses.
Modeling Trustworthiness	Provides evaluation criteria for model verification and validation.
Security as a Functional Requirement	Provides systematic identification and justification of needed security capabilities as functional requirements.
Security Orchestration	Provides discussion and value framework for considering nature and degree of autonomous security responses and actions.
Collaborative Mutual Protection	Provides discussion and value framework for considering nature and degree of collaborative mutual protection strategy.
Architectural Agility	Provides capability-based framework for security strategy with feature-based variations.
Operational Agility	Provides loss-driven framework for response strategy with feature-based variations.
Education and Competency Development	Provides means for educators and engineers to explore system security engineering at the strategy level independent of detailed tactical methods.

Though there is a literature base espousing methods for achieving stakeholder alignment on understandable security requirements, those methods have not become standard practice. As a result, and in follow on to this paper's kickstart, INCOSE's Systems Security Engineering working group has accepted the challenge to develop a compelling and embraceable method. Work starting in 2023 intends to develop a loss-driven, needs-oriented, capability-based security requirements engineering product, one with a high-level transdisciplinary framework of:

1. Needs – Loss-driven problems to solve
2. Goals – Desired outcomes expressed as capabilities
3. Strategies – High-level requirements
4. Tactics – Security system functional requirements

Recognizing that "the future is already here, it is just not evenly distributed" (often attributed to fiction writer William Gibson), it is worth noting that an existing approach that is most strongly consistent and supportive of a loss-driven, needs-oriented, capability-based security strategy is System-Theoretic Process Analysis for Security, or STPA-Sec (Young & Leveson, 2014).

STPA-Sec pushes for a security strategy outlined by needs (the problem to solve) independent of solution knowledge and resources. It calls for a reframing of the usual security problem: "Just as STAMP (System-Theoretic Accident Model and Processes) reframes the safety problem as a control rather than a failure problem, applying STAMP to security involves reframing the security problem into one of strategy rather than tactics" (Young & Leveson, 2014). The STPA-Sec process identifies top-level losses of stakeholder concern early, recognizing the need to control loss and deliver capability (Young, 2020).

STPA-Sec is, at best, a partial answer; more work is needed. Some of the best of GORE and SQUARE may provide more of the response and some of the practices required.

A supporting effort of further work involves research on the cost and effect of misalignment and the cost/benefit ratio of alignment to motivate efforts further and inform priorities. Such research will encourage and prioritize actions to further develop and identify security alignment practices and methodologies, including identifying case studies of successful practices.

References

Dove, R., K. Willett, T. McDermott, H. Dunlap, D. P. MacNamara, and C. Ocker. 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

Horkoff, J., F. Basak Aydemir, E. Cardoso, T. Li, A. Mate, E. Paja, M. Salnitri, L. Piras, J. Mylopoulos, and P. Giorgini. 2017. Goal-Oriented Requirements Engineering: An Extended Systematic Mapping Study. Requirements Engineering, Springer. https://link.springer.com/content/pdf/10.1007/s00766-017-0280-z.pdf

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

Ross, R., M. Winstead, M. McEvilley. 2022. Engineering Trustworthy Secure Systems. NIST Special Publication 800-160v1r1. National Institute of Standards and Technology, Gaithersburg, MD. November. https://doi.org/10.6028/NIST.SP.800-160v1r1

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

van Lamsweerde, A. 2001. Goal-Oriented Requirements Engineering: A Guided Tour. Proceedings Fifth IEEE International Symposium on Requirements Engineering, doi: 10.1109/ISRE.2001.948567. https://www.info.ucl.ac.be/~avl/files/RE01.pdf

Watson, M., B. Mesmer, G. Roedler, D. Rousseau, J. Calvo-Amodio, C. Keating, W. D. Miller, S. Lucero, R. Gold, C. Jones, D. Long, R. W. Russell, and A. Sedmak. 2022. *Systems Engineering Principles*. INCOSE Technical Product, International Council on Systems Engineering.

Wheatcraft, L., T. Katz, M. Ryan, and R. Wolfgang. 2022. *Needs and Requirements Manual*. INCOSE-TP-2021-002-01 | VERS/REV: 1.1 | May 2022.

Young, W. and N. G. Leveson. 2014. An Integrated Approach to Safety and Security Based on Systems Theory. Communications of the ACM, Vol. 57 No. 2, pps 31-35, February. http://sunnyday.mit.edu/papers/cacm232.pdf

Young, W. 2020. Basic Introduction to STPA for Security (STPA-Sec). Tutorial at the 2020 System-Theoretic Accident Model and Processes (STAMP) Workshop July 2020. http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/STPA-Sec-Tutorial.pdf

Acknowledgement

Gary Stoneburner, a senior system security engineer and member of the senior professional staff of the Johns Hopkins Applied Physics Laboratory, contributed to the discussions that resulted in this paper's content.

Biography

Rick Dove is an independent operator specializing in systems security and agile systems engineering, strategy, and research. He chairs the INCOSE working groups for Systems Security Engineering and for Agile Systems and Systems Engineering. He is an INCOSE Fellow, and leads the Systems Security topic area for INCOSE's Future of Systems Engineering (FuSE) initiative.

Dr. Mark Winstead is a Principal Systems Security Engineer with The MITRE Corporation. He is active in both the Systems Security Engineering and Resilient Systems Working Groups and taught multiple tutorials at INCOSE conferences on systems engineering role in security. He also coauthored NIST SP 800-160 Volume 1 Revision 1 Engineering Trustworthy Secure Systems.

Holy Dunlap is a Principal System Security Engineer, Cyber Supply Chain Risk Management Technical Advisor with MITRE Labs Cyber Solutions Innovation Center. She has +20 years of Defense Industry Prime experience. As the past NDIA Systems Engineering Division chair, she has led collaboration with government, industry, FFRDC, and academia.

Matthew Hause is a Principal at SSI, a co-chair and INCOSE member of the UAF group, and member of the OMG SysML team. He has been developing multi-national complex systems for almost 45 years as a systems and software engineer. He has authored over 100 technical papers on MBSE, SoS, UAF/UPDM, SysML, etc., and is the recipient of the MBSE Propellor Hat award.

A. Scalco holds a Ph.D. in SYSE (2022), M.ENG. (2012), and MBA (2009). She is a member of INCOSE Institute for Technical Leadership and Certified Systems Engineering Professional (CSEP). She is an Institute of Electrical and Electronics Engineers (IEEE) Senior Member, and Information Technology Infrastructure Library (ITIL) IT Service Management Expert Certified.

Dr. Keith Willett is a senior systems engineer for the US Dept of Defens**e**. He co-chairs the INCOSE working groups for Systems Security Engineering and for Agile Systems and Systems Engineering. Dr. Willett's most recent publication contributions are *The Handbook of Security Science* and *Disruption, Ideation, and Innovation for Defense and Security,* Springer Publishing.

Dr. Adam David Williams is a Principal R&D Systems Engineer in the Center for Global Security and Cooperation at Sandia National Laboratories. Dr. Williams is a subject matter expert on cyber-physical nuclear systems, complex risk in the security applications, and innovative solutions to uncertain global security challenges.

Dr. Beth Wilson is an Adjunct Professor at Worcester Polytechnic Institute after retiring from Raytheon where she worked for 33 years. She is an INCOSE Expert Systems Engineering Professional (ESEP), INCOSE Certification Advisory Group (CAG) chair, and co-chair for the INCOSE Systems Security Engineering working group.