



33rd Annual **INCOS**
international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023



Roundtable explores how security joins performance and safety as foundational systems design perspective

IS23 Roundtable

Monday 17-July, 13:30-15:00

Dr. Dawn Beyer dawn.m.beyer@lmco.com
Rick Dove dove@parshift.com
Tom McDermott tmcdermo@stevens.edu
Mark Winstead mwinstead@mitre.org

Download this file: www.parsift.com/t/p2.pdf

Roundtable Context

**“~~Cyber~~Security will be as foundational a perspective in systems design
as system performance and safety are today.”**
(INCOSE’s Vision 2035, page 37)

**No argument is heard against the value of this;
but how will it come to pass?**

Is this wishful thinking or feasible outcome?

**This roundtable will explore the what, why, and how of this expectation
as a practical Systems Engineering responsibility.**

=====

This Roundtable is part of a FuSE Security project-in-process

Roundtable

Instigation, Illumination, Collaboration

Roundtable Purpose:

- **Socialize the need.**
- **Broaden the collaboration.**
- **Accelerate engagement.**

Instigators will kick-start,

but we're all in this together.

Instigators

Dr. Dawn Beyer: Dr. Dawn Beyer is a Lockheed Martin (LM) Senior Fellow. She led the development and implementation of the LM Cyber Resiliency Level® framework as a standard way to measure cyber resiliency maturity. Dr. Beyer recently led the development of the 2022 LM Cyber Defense Technology Strategy. She is currently leading the independent research and development project CyCADA™--Cyber intelligence Capabilities for Autonomous Detection & Defeat of Attacks, an end-to-end cyber ecosystem of cyber resiliency capabilities.

Rick Dove: Founder and chair of the INCOSE Systems Security Engineering working group. Lead for the Security Topic under INCOSE's Future of Systems Engineering (FuSE) initiative. Previously principle investigator, architect, and strategist for multiple DHS and Army Small Business Innovative Research security projects; and CISO for Silterra semiconductor fabrication facility.

Tom McDermott: Chief Technology Officer of the Systems Engineering Research Center (SERC) and a faculty member in the School of Systems and Enterprises at Stevens Institute of Technology. With the SERC he develops new research strategies and is leading research on digital transformation, model-based security, and artificial intelligence applications. He previously was Faculty and Director of Research at Georgia Tech Research Institute where he founded the GTRI cybersecurity research lab; and as Director and Integrated Product Team Manager at Lockheed Martin where he led development of the F-22 secure computing systems.

Mark Winstead: 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.

Background

**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.

Systems engineering has responsibility for identifying system design requirements.

**Discovering system security design requirements
as loss-driven, needs-oriented capabilities does not require technical security expertise.**

**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.**

**This avoids the issue of scarce security expertise and defines a viable approach
for security joining performance and safety as foundational systems design perspectives.**

Security will be as foundational a perspective in systems design as system performance and safety are today

Today's Questions...

Q1: Why is this a necessary path?

Q2: Why is this not the case already?

Q3: What is needed to make this the case?

90 Minute Plan

9 mins: Context

12 mins: Q1 x 4 seeds

15 mins: Community

12 mins: Q2 x 4 seeds

15 mins: Community

12 mins: Q3 x 4 seeds

15 mins: Community

**Security will be as foundational a perspective in systems design
as system performance and safety are today**

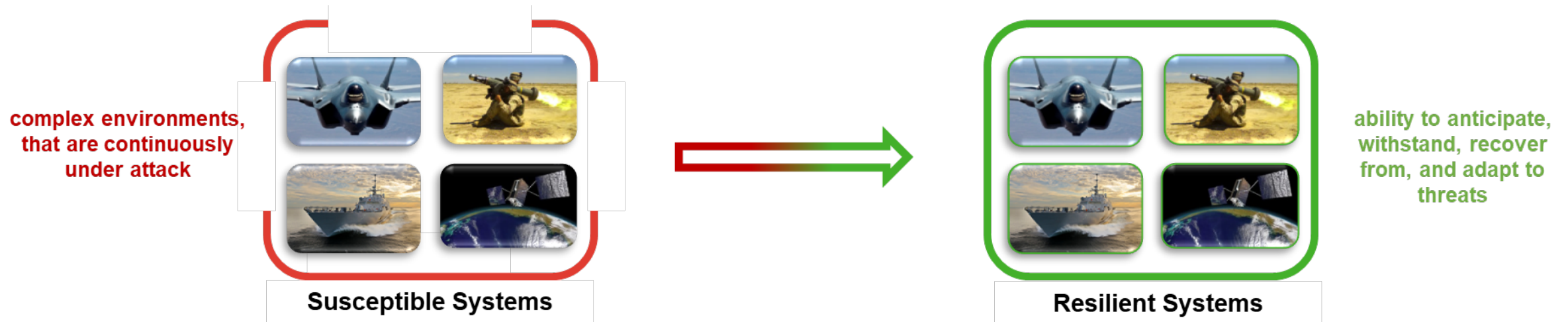
#1: Why is this a necessary path?

#2: Why is this not the case already?

#3: What is needed to make this the case?

Why is this a necessary path?

Dawn Beyer



Problem

The 1) deficiency in risk awareness coupled with 2) technology changes within complex environments, that are 3) continuously under attack, make measuring cyber resiliency a hard problem.

Solution

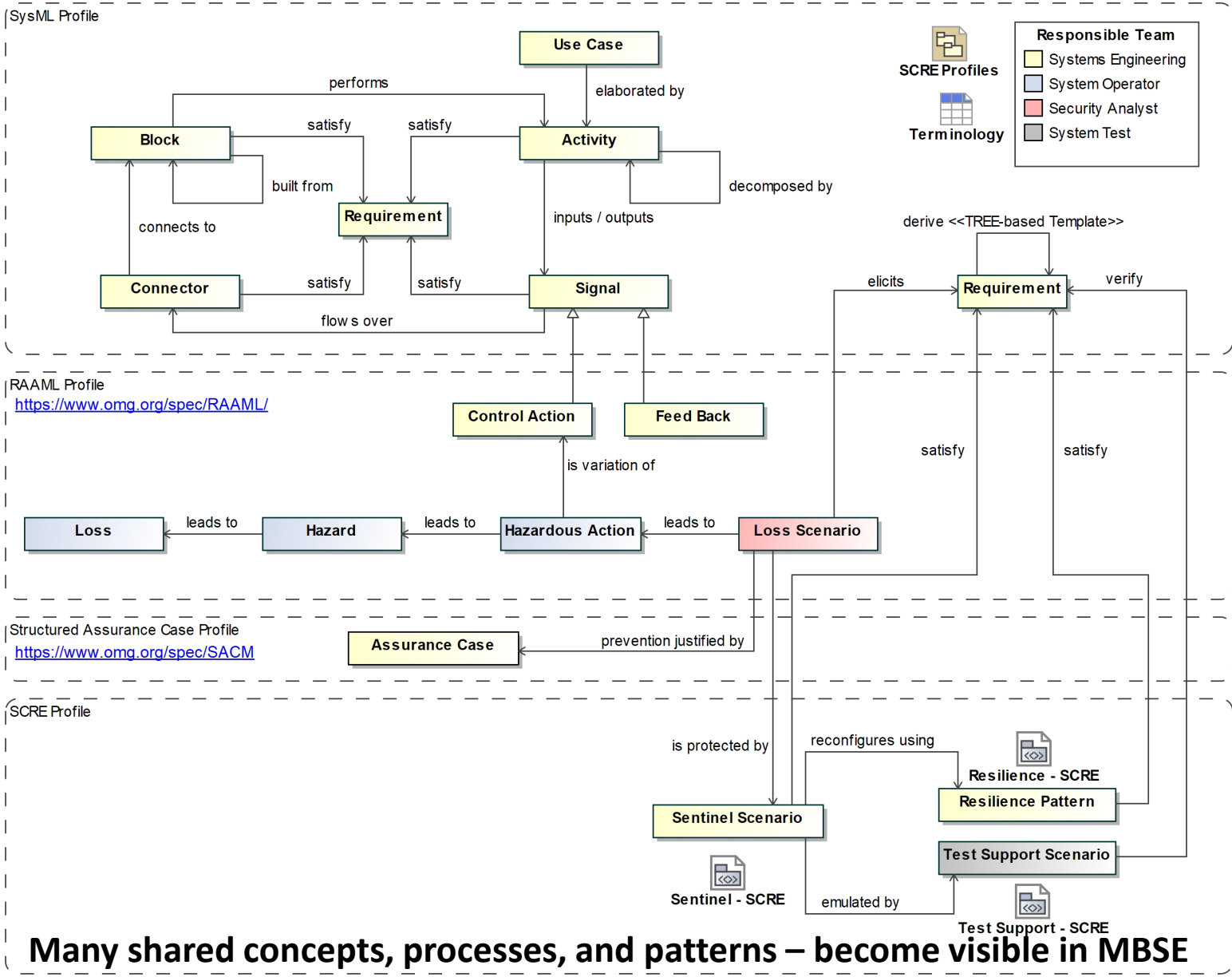
A framework that enables programs to **employ common risk- and engineering-based approaches** to measure cyber resiliency and manage cyber risk of systems.

© 2023 Lockheed Martin Corporation. All Rights Reserved.

Secure Cyber-Resilient Engineering (SCRE) MBSE Metamodel and Process

SCRE Modeling Tasks: 5-step process

- 1A - Identify Operational **Use Cases** for *Communication* focus (Problem Framing).
- 1B – Define Activity Diagrams (**Block, Connector, Signal**) to realize Communication Use Cases
- 1C – Define Control Structure (**Control Action, Feedback**) to support Communication Use Cases
- 2 – Perform Hazard Analysis (**Loss, Hazard, Hazardous Action**) for Communication Control Structure
- 3 – Identify **Loss Scenarios** for Control Structure & Risk Assessment
- 4 – Define Shadow Resilience Architecture (**Sentinel Scenario, Resilience Pattern, SCRE Requirements**) for Loss Scenarios to be ‘protected against’. Define **Assurance Cases** for Loss Scenarios to be ‘prevented’.
- 5 – Define Shadow Resilience Test & Evaluation (**Test Support Scenarios**) to verify SCRE Requirements



**The Anderson Report in 1972 concluded its necessity:
“Unless security is designed into a system from its inception, there is little chance that it can be made secure by retrofit ...”**

From Information Assurance Technical Framework (2002) “Nothing is more inefficient than solving the wrong problem and building the wrong system ... :

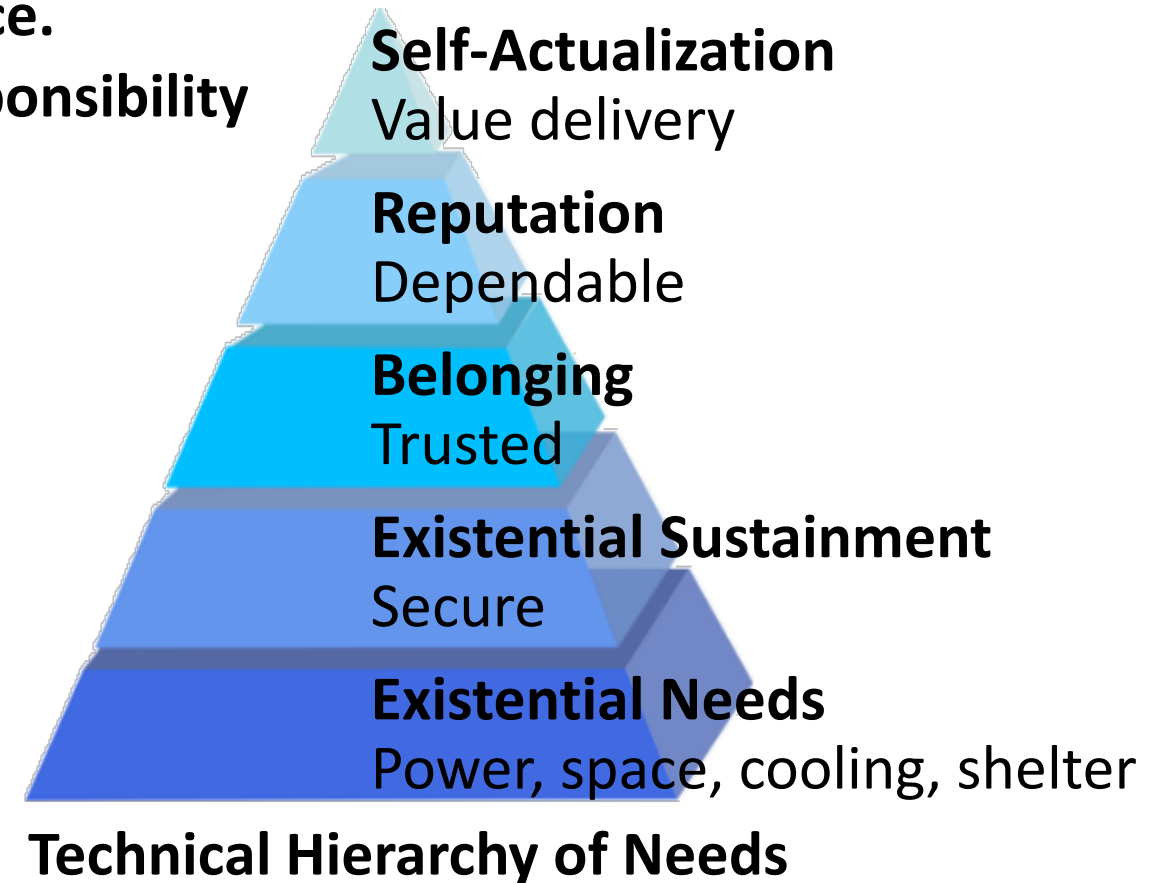
1. Always keep the problem and solution spaces separate.
2. The problem space is defined by the customer’s mission or business needs.
3. The systems engineer ... defines the solution space, driven by the problem space.”

The need is for strategic thinking up front, with systems to be inherently securer, such as use of security design order of precedence (NIST SP 800-160 Vol 1 Section D.3). Such thinking must occur while the foundations are being poured

Why is this a necessary path?

Rick Dove

- System functionality is under increasing existential threat.
- Performance & safety require a live viable system.
- Stayin' alive takes precedence over performance.
- It gains Systems Engineering attention and responsibility for the security of systems.



**Security will be as foundational a perspective in systems design
as system performance and safety are today**

Community Question:

#1: Why is this a necessary path?

#2: Why is this not the case already?

#3: What is needed to make this the case?

Security will be as foundational a perspective in systems design as system performance and safety are today

#1: Why is this a necessary path?

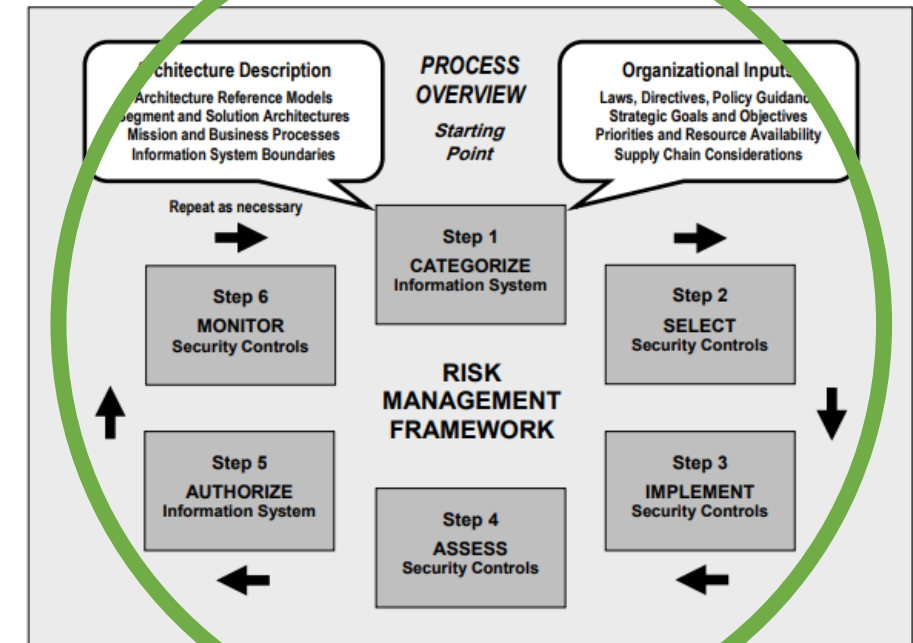
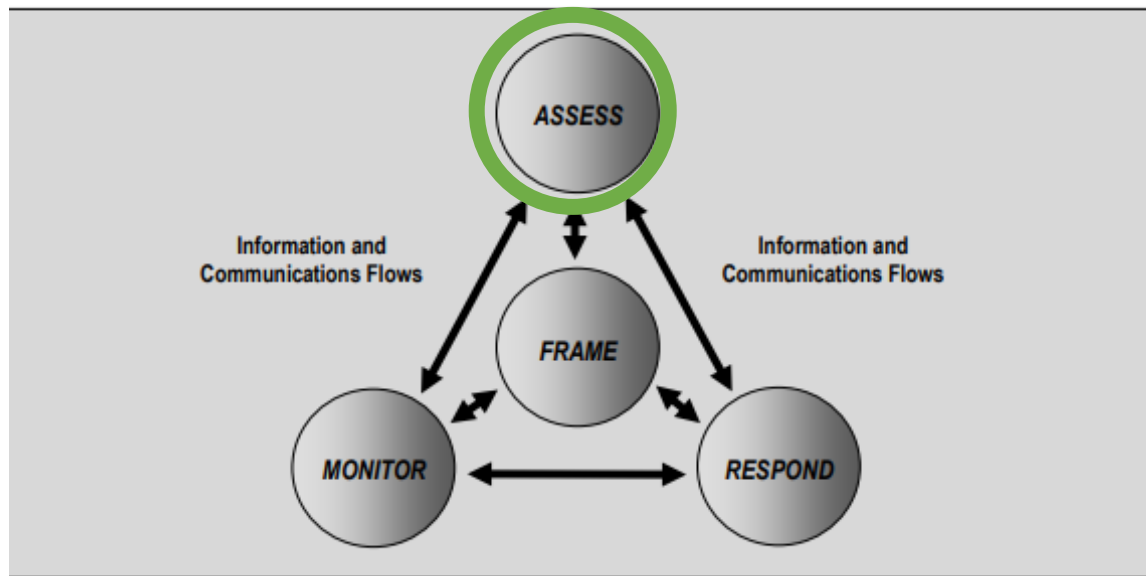
#2: Why is this not the case already?

#3: What is needed to make this the case?

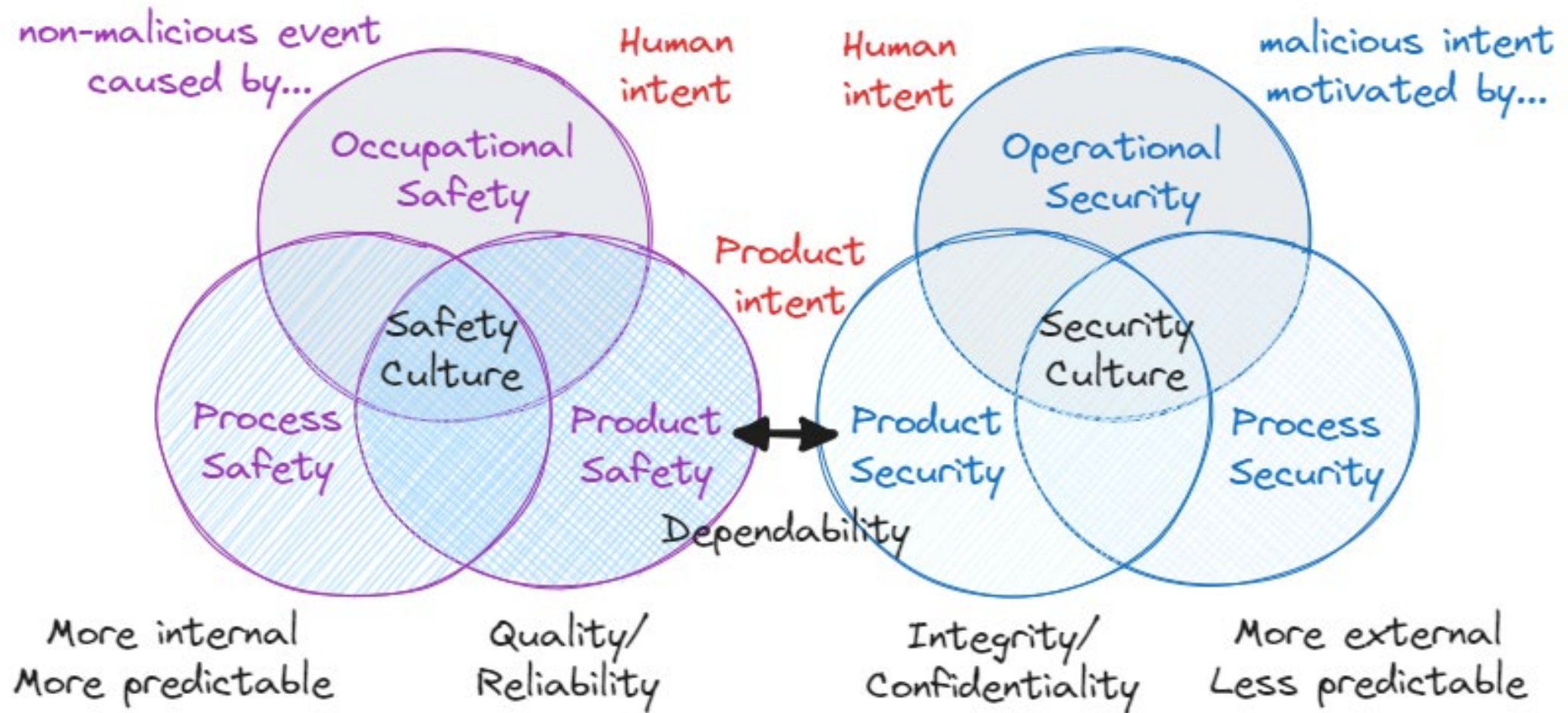
Why is this not the case already?

Dawn Beyer

- Cost to Mitigate Risks
- Deficiency in Information Sharing of CTI and DM (challenges: classified; special access programs)
- Shortage of Systems Security Engineering SMEs—Security is Everyone's Responsibility
- Insufficient Budget for Effective Training; Cost/Benefit Analysis of CoAs



Why is this not the case already? **Not many organizations are effectively integrating safety and security cultures together. Or SE cultures in general. Good SE can be the integrator.**
Product focus will always be the primary driver.



Barriers:

- 1) Economics – get it out the door. Pay the security bill later.
- 2) Prescriptive approaches, especially applied after design started – solution-based thinking.
- 3) Thinking of security as countering threat, not assuring delivery or addressing concerns – driven by tactical thinking.

Baking chocolate into a cake does not make it a chocolate cake;

Baking in security does not make a system secure

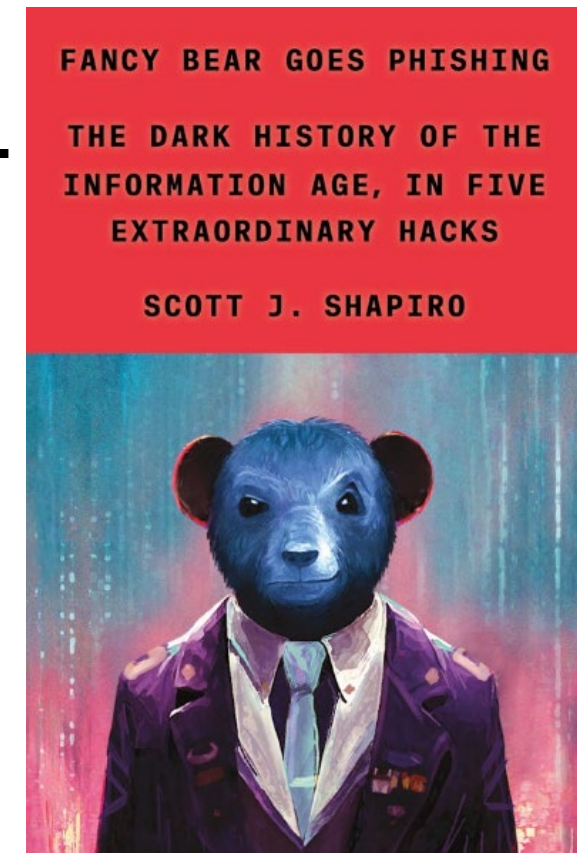


“A productive way to view security is as a concern ... But it’s not uncommon to come across situations where security is described as a set of features. The difference is that even when security features address a specific security problem, your concern about security may not have been met.” Johnsson, Deogun, & Sawano, Secure By Design, 2019

Why is this not the case already?

Rick Dove

- Insufficient incentives, inadequate skills, inadequate funding.
- Law will not hold system creators accountable for harm caused by inadequate security.
- Contracted development doesn't require this.
- It is a socio-cultural issue, treated as a technical issue.
- **"Giving information to people is not a good way to change behavior. If we want to change behavior we have to change the environment. Reduce the friction and add motivation."**
- **Offering strategies can work when decision makers are looking for a way to accomplish something. This is not the general situation we are facing (but finding some exceptions would be useful).**



**Security will be as foundational a perspective in systems design
as system performance and safety are today**

Community Question:

#1: Why is this a necessary path?

#2: Why is this not the case already?

#3: What is needed to make this the case?

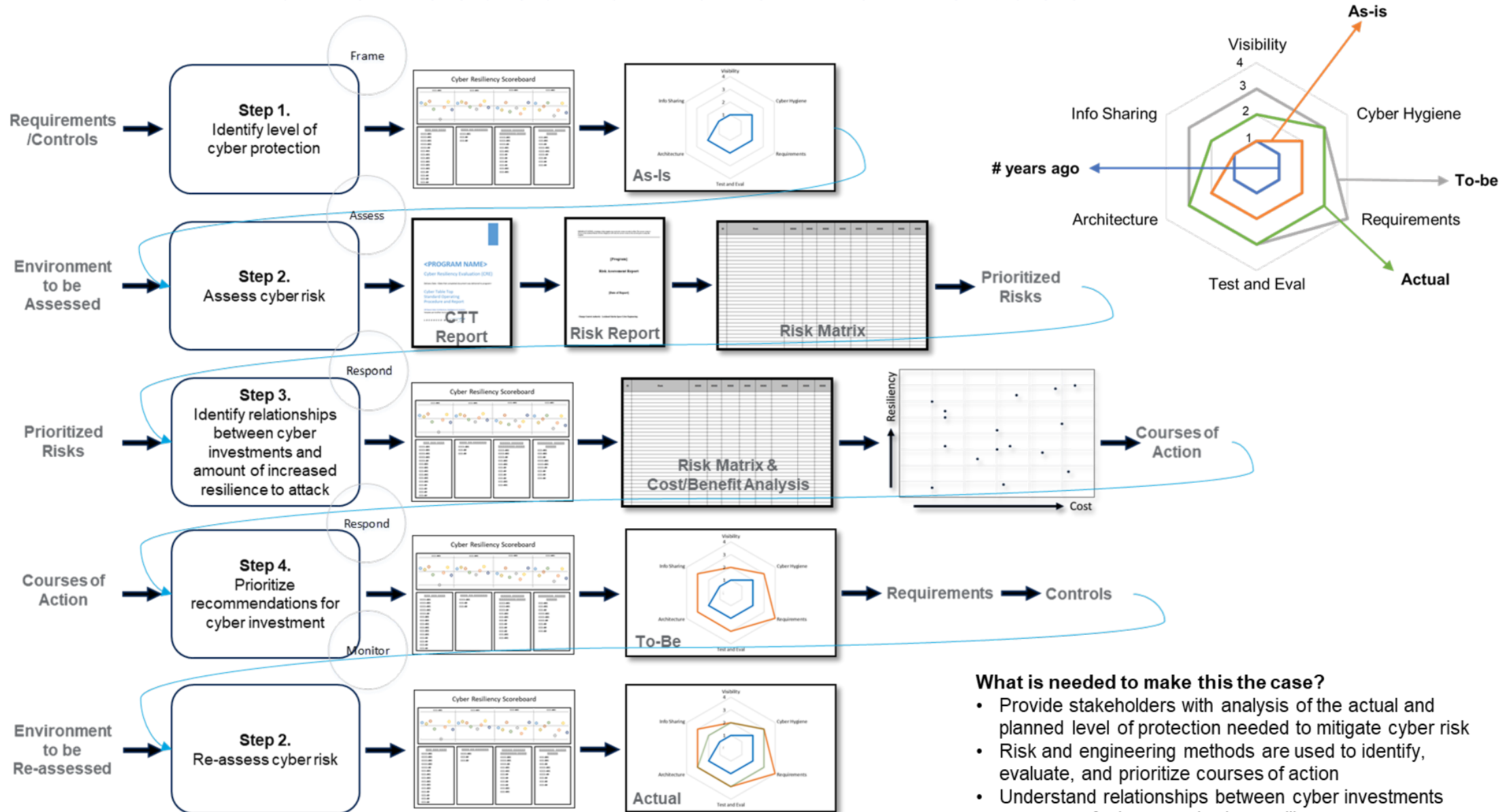
Security will be as foundational a perspective in systems design as system performance and safety are today

#1: Why is this a necessary path?

#2: Why is this not the case already?

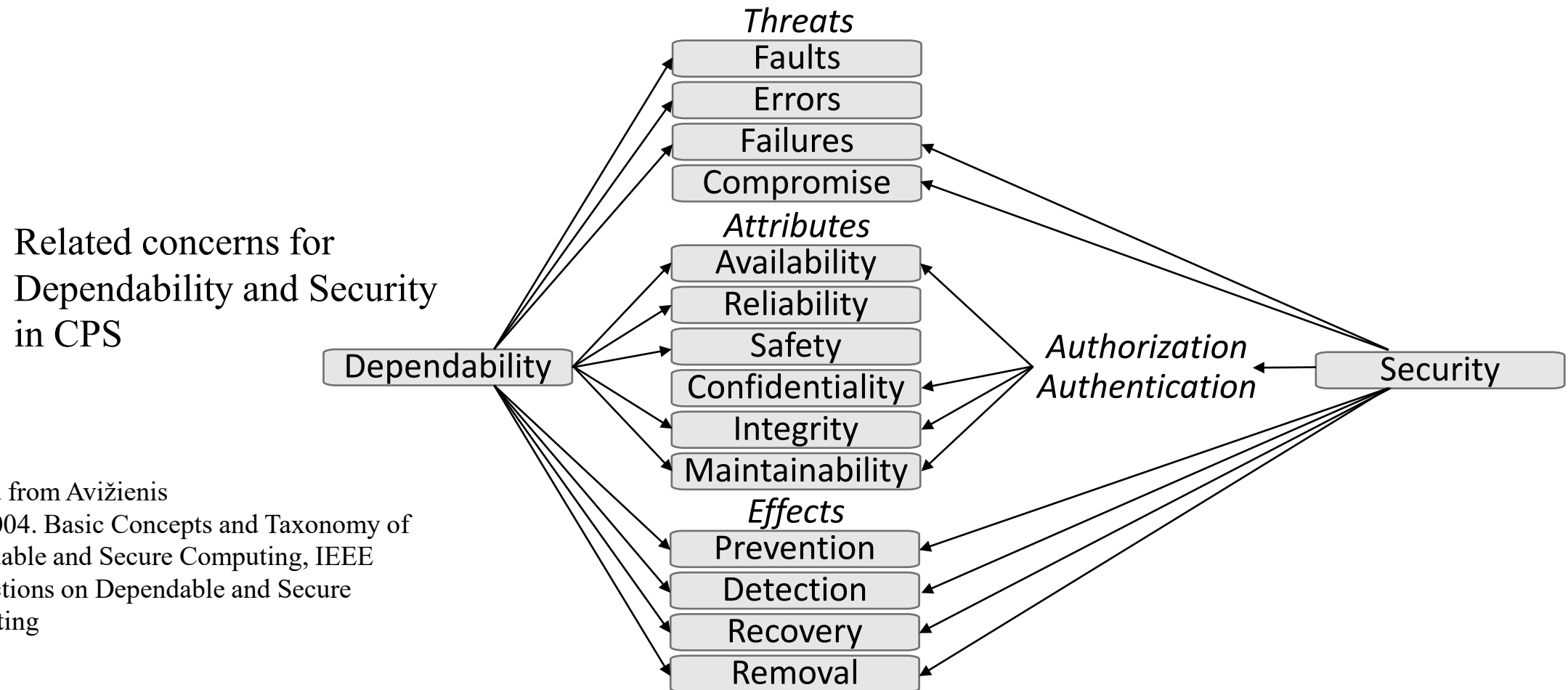
#3: What is needed to make this the case?

What is needed to make this the case? Dawn Beyer



© 2023 Lockheed Martin Corporation. All Rights Reserved.

The SE community must stop treating concepts like security, safety, reliability, etc. as independent processes and take advantage of MBSE to integrate these.



adapted from Avižienis
et al, 2004. Basic Concepts and Taxonomy of
Dependable and Secure Computing, IEEE
Transactions on Dependable and Secure
Computing

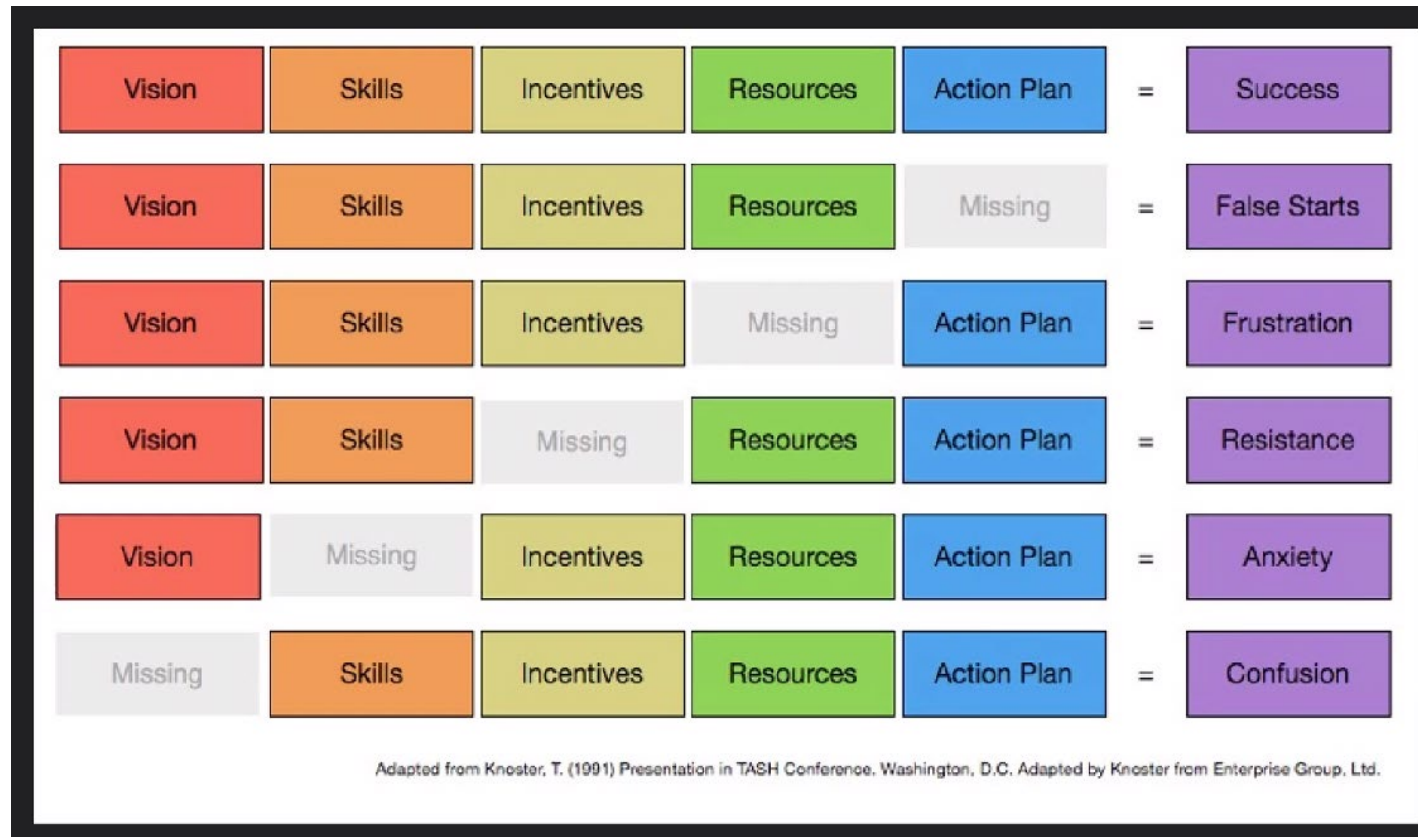
Advancing systems engineering overall

Viewing security as achieving *authorized* and *intended* behaviors and outcomes, including not experiencing intolerable effects of loss – security of the intended functionality.

Embrace transdisciplinary – security as freedom from loss of assets with unacceptable consequences – where asset is anything of value to a stakeholder – system capability (resilience/survivability), humans (safety/privacy/survivability), information/data (“cyber”), etc.

What is needed to make this the case? Rick Dove

- Required by the market (contract and commercial).
- Research-based economic argument.
- Democratizing security with needs-oriented, loss-driven, capability-based security requirements engineering.
- Vision + Skills + Incentives + Resources + Action Plan = Success



**Security will be as foundational a perspective in systems design
as system performance and safety are today**

Community Question:

#1: Why is this a necessary path?

#2: Why is this not the case already?

#3: What is needed to make this the case?

Background Position Statements

Rick Dove Position Statement

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 expectations.

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 feeling as both necessary and useful.

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.

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 same needs.

Systems engineering has responsibility for identifying system design requirements. Discovering, expressing, and aligning system security design requirements as loss-driven, needs oriented capabilities does not require technical security expertise and serves as a focal point for stakeholder alignment. This avoids the issue of scarce security expertise and defines a viable approach for security joining performance and safety as foundational systems design perspectives.

Dawn Beyer Position Statement

Cybersecurity should already be foundational in systems design as system performance and safety are today. We have processes, practices, and tools to achieve this.

However, there aren't enough cybersecurity subject matter experts to fill the demand. Skills shortage not only makes recruitment and retention harder; but also, leads to employee burnout and an increase in voluntary attrition.

Therefore, in order for cybersecurity to successfully be as foundational in systems design as system performance and safety are today, cybersecurity should be everyone's responsibility, like safety.

In addition to workforce challenges is the deficiency in risk awareness and management. Most organizations and programs don't continuously identify, assess, and mitigate security risks.

Stakeholders need assistance with prioritizing risks and selecting courses of action based on their risk tolerance.

Decision makers need assistance with understanding how their investments mitigate risk and increase cyber resiliency

Tom McDermott Position Statement

INCOSE's Vision 2035, posits that "Cyber-security will be as foundational a perspective in systems design as system performance and safety are today." Systems are increasingly composed of heterogeneous elements, both cyber and physical in nature. While this coupling can produce capabilities beyond those achievable before, it also makes these systems vulnerable to classes of threats previously not relevant for many physical control and computational systems. What is unique to cybersecurity in systems design is the notion of sentient external threats. While natural threats may loosely be addressed via measures of reliability or integrity, sentient threats (i.e., security) are external to the system in question. What is not unique is the system functions we define to counter these, they can be reused to equally produce security, safety, integrity, and similar outcomes. The discipline of cybersecurity has for too long tried to just prevent these threats from entering the system. Systems engineering must stand up to provide holistic understanding and modeling of the threat behaviors within the system, and the system's response, which is generally referred to as cyber resilience. Cybersecurity in this vision and perhaps security in general are too narrowly focused terms. A comprehensive approach involves many non-functional requirements: security, safety, integrity, maintainability, assurance, etc. All of these must be linked in an analytical framework to determine if a system is protected to some level of acceptable risk versus cost. Likewise, the approach can and should draw on multiple specialty disciplines including security, safety, reliability, integrity, maintainability and assurance.

Current research conducted by the Systems Engineering Research Center (SERC) is directly in support of this vision. The research applies a systems engineering approach to the concepts of cyber resilience in operational settings of a system. Cyber resilience may be achieved through any number of implementable techniques that provide capabilities to respond to threats. These techniques may be represented as design patterns, each contextually relevant to a given threat type, and are ideally reusable from one system to another. Security is realized by incorporating these design patterns into the system, thereby generating an adapted system architecture with new or improved, threat-specific capabilities. The set of selected security design patterns form the security architecture.

The SERC's System Aware Security work has explored the representation of both system behaviors and threat behaviors in formal MBSE representations, specifically in SysML. Unlike system assurance, which by its nature requires a complete system design, and cybersecurity, which treats a system as a black box, the system resilience approach offers the ability to analyze cyber threats and system design protections early in and throughout the systems engineering process. Because we define in terms of system behaviors, it is possible to reason about systems resilience in terms of system functions in advance of a design. In other words, across the full SE lifecycle. A principal focus of the SERC has been the development of methods and tools that support functional system design for cyber resilience in cyber physical systems. The objective of these efforts was to develop and transition an end-to-end systems engineering methodology intended to close the loop between mission level resilience analysis and system development activities using digital engineering and MBSE oriented processes. They have been developed in a research setting but are now being applied into new defense-related systems and industrial control environments.

So yes, it will come to pass if the SE community stops treating concepts like security, safety, reliability, etc. as independent specialty disciplines and takes advantage of MBSE to integrate these across the SE process. The SERC has demonstrated the methods and is beginning to apply them widely.

Mark Winstead Position Statement

Historically, cybersecurity has the tendency to be bottoms-up – how can a malicious threat find and exploit vulnerabilities, and what effect they can generate as a result. Cybersecurity is practiced by specialists using their own language and jargon, not as a general competency of other fields nor sufficient cross-pollinating with other fields. Insufficient focus has occurred for a systems-driven top-down thinking.

To be a foundational perspective in systems design like performance and safety, systems engineering's cybersecurity perspective needs to be systems-driven, top-down perspective. Moreover, the perspective needs to align to performance and safety in ways enabling more transdisciplinarity and relate better to all stakeholders.

Achieving these are not exclusive of one another.

Safety is often defined in terms of avoiding loss or endangerment of human life or limb or the environment. NIST SP 800-160 Volume 1 Revision 1 expresses security in terms of loss by defining security as freedom from the conditions that can cause loss of assets with unacceptable consequences. By approaching security from a loss/consequences/effects approach to security including cybersecurity, I believe doors open for new transdisciplinary thinking not just with safety but reliability and other loss concerned disciplines as well.

This loss thinking approach opens the aperture for a top-down approach and to relating to stakeholders. Systems engineering begins with stakeholder needs – a problem needs addressing. The need itself may be dealing with loss itself, but more commonly, in expanding the need statement derivative needs related to loss are identified – a capability needs to be delivered without unacceptable degradations (a form of loss), the users of the solution need to be free of harm (a loss avoided), etc. As the solution moves to realization, new derived needs are identified, such as the need for integrity of system data (no loss of integrity). The stakeholder's real need is not with the adversity itself but the effect or loss the adversity may trigger or create.

Furthermore, such a perspective should be less focused by reacting to known or possible specific threat actions, but more focused on assurance (sufficient grounds for confidence) in the face of adversity. The need is to think about ensuring delivery of the desired system capability despite failure that may occur, where the failure may be a reliability shortfall, operator error, or malicious activity (any reliability shortfall may be a result of malicious activity). Systems engineering perspective needs to be driven by “when things go wrong” first, as for complex systems and intelligent adversaries no realistic bound exists on “why”.

This assurance needs to be driven by two capabilities the systems engineer should focus to, capabilities core for any system to control loss and loss effects. One is *complete mediation*, that any interaction, behavior, and outcome is authorized following documented intent; the other is *system control*, that system interactions, behaviors, and outcomes are only what is intended. Complete mediation and system control are intended as enabling capabilities to meet stakeholder needs – ensuring the system delivers the performance capability needed within stakeholder other needs such as operating safely.