USD(R&E)

Risk and Issue Revisited in Systems Security Engineering

Dr. Mark Winstead
Principal Chief Engineer, Systems Security
The MITRE Corporation
National Defense Industrial Association Systems and Mission Engineering Conference
November 1-3, 2022

Summary

- Much of what some security/cybersecurity/resilience communities refer to as “risk” deal more with operational rather than engineering risk.
- The subsequent approaches may cause dissonance with systems engineering efforts, leading to misapplication of resources and efforts.
- This presentation provides an examination of technical protection risks and issues and the opportunity presented to better align with systems engineering needs and equities by adopting different approaches.
- These possible alignments are reflective of how safety risk aligns with systems in communities with similar objectives due to the catastrophic consequences associated with system failure.

Some Systems Engineering Definitions

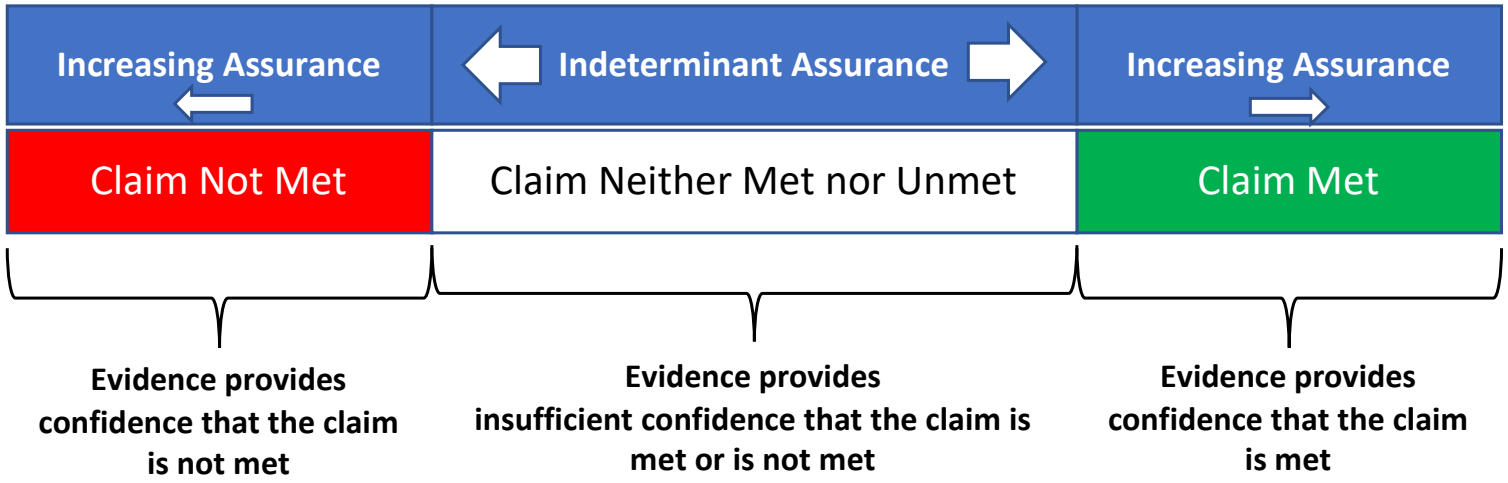
- **Risk:**
  - Effect of uncertainty on objectives – ISO 73
  - Effect: deviation from the expected
- **Technical risk:**
  - Potential for performance deficiencies (NASA Systems Engineering Handbook, adapted)
- **Technical protection risk:**
  - Potential for protection performance deficiencies (as informed by protection expectations /requirements)
- **Issue:**
  - Event or condition with negative effect that has occurred (such as a realized risk) or is certain to occur (probability = 1) – DoD Risk, Issue, and Opportunity Guide
  - Systems Engineering Body of Knowledge definition refers to types of issues: A problem that exists, a risk certain to occur, and a lack of information

Definitions of the terms we use are necessary for effective communications. There is no right or wrong definition, only the one we choose to use. … Limited definitions, however, may also limit potential solutions to the problems. If we start from more inclusive and practical definitions, then overlap and common approaches to achieving the properties are possible.

- Nancy Leveson, "Safety and Security are Two Sides of the Same Coin," **The Coupling of Safety and Security**

Assurance

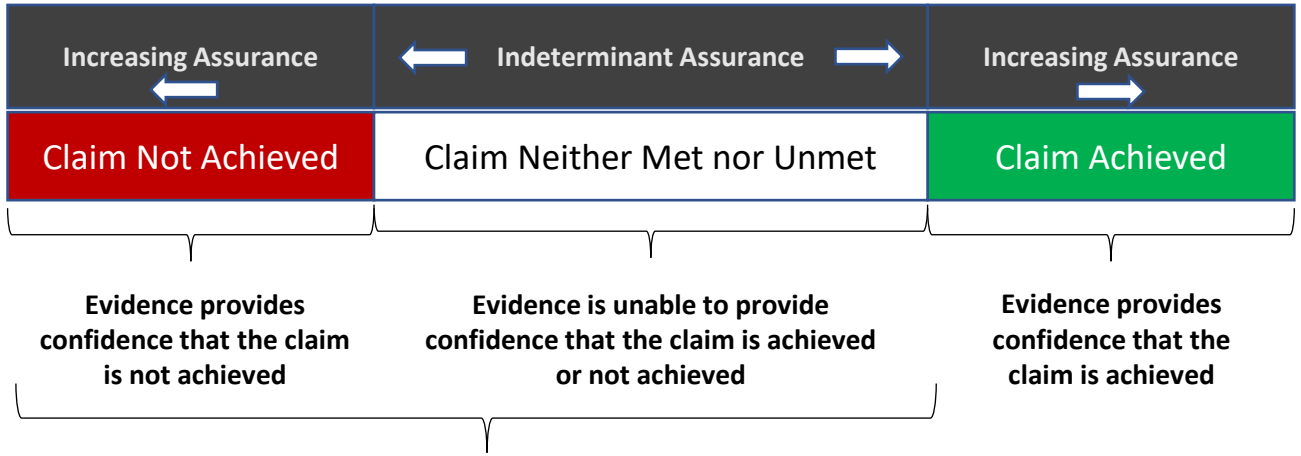
- **Assurance is grounds for justified confidence a claim has been or will be achieved [IEEE 15026]**
  - Assurance – certainty
  - Lack of assurance – uncertainty
- **Three possibilities**
  - Sufficient grounds that a claim is achieved
  - Sufficient grounds that a claim is not achieved
  - Insufficient grounds to support any conclusion about a claim
- **Claims of concern for this presentation**
  - "Required performance will be delivered"
  - "Required protection performance will be delivered"



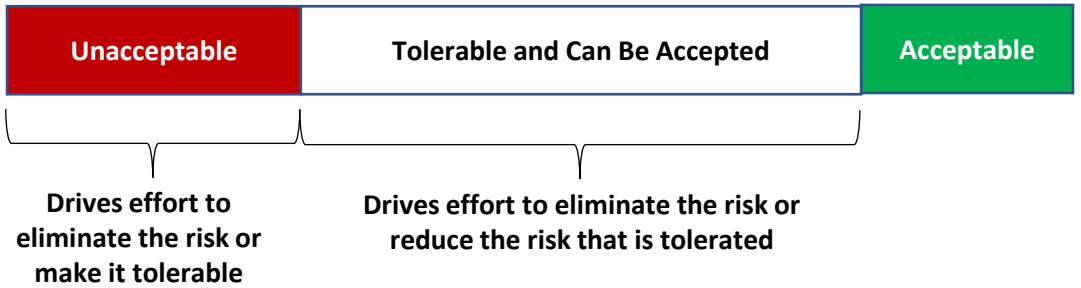
Deficiencies and Risk

ASSURANCE

RISK



Analysis to translate the assurance deficit into risk



Risk Management Effort

Assurance Activities

For risk driven by confidence derived from evidence-based judgments

1. Determine how much confidence is needed
2. Acquire the confidence

If

(a) The confidence needed is met by the confidence acquired – good!

(b) The confidence needed is not met by the confidence acquired – take action!

Risk Management Activities

1. Translate the deficit in confidence into the associated risk(s)
2. Determine if the associated risk is
   - Unacceptable
   - Tolerable and acceptable
   - Non-existent
3. Conduct the appropriate risk management activities to identify, assess, and accept or mitigate the identified risks

Technical Protection Information Deficiencies Are Critical Issues

- **Information often used/discussed includes threat, vulnerability, and undesired effects (undesired losses and consequences)**
- **Deficiencies exist in threat information**
  - Timeliness, accuracy, completeness, actionability, etc.
- **Deficiencies exist in vulnerability information**
  - Supply chain insight gaps (e.g., use of Commercial Off-The-Shelf)
  - Deficiencies in engineering rigor result in vulnerability information deficiencies
- **Deficiencies exist in undesired losses and consequences information**
  - Typically, a result of deficiencies in engineering process and rigor

Which deficiencies are easier to address? Harder to address?

Threat, Vulnerability, and Effect Information Deficiency Handling

- **Threat and vulnerability are intractable; undesirable consequences of effects bounded**
- **Through rigor in engineering efforts, it is possible to sufficiently close effect information deficiencies**

Threat and Vulnerability

What might/has happened?

- Incomplete data on threat and vulnerability make this always incomplete
- A constant chase of the OODA loop

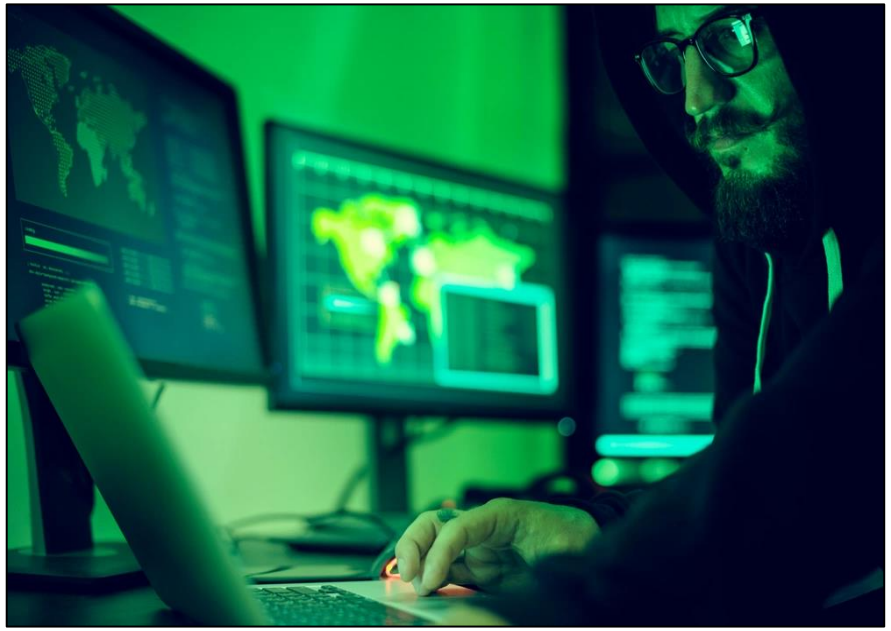
Effects

What is our confidence in addressing what might be or is?

- Ensuring function
- Effective means to verify action to control loss and loss effects

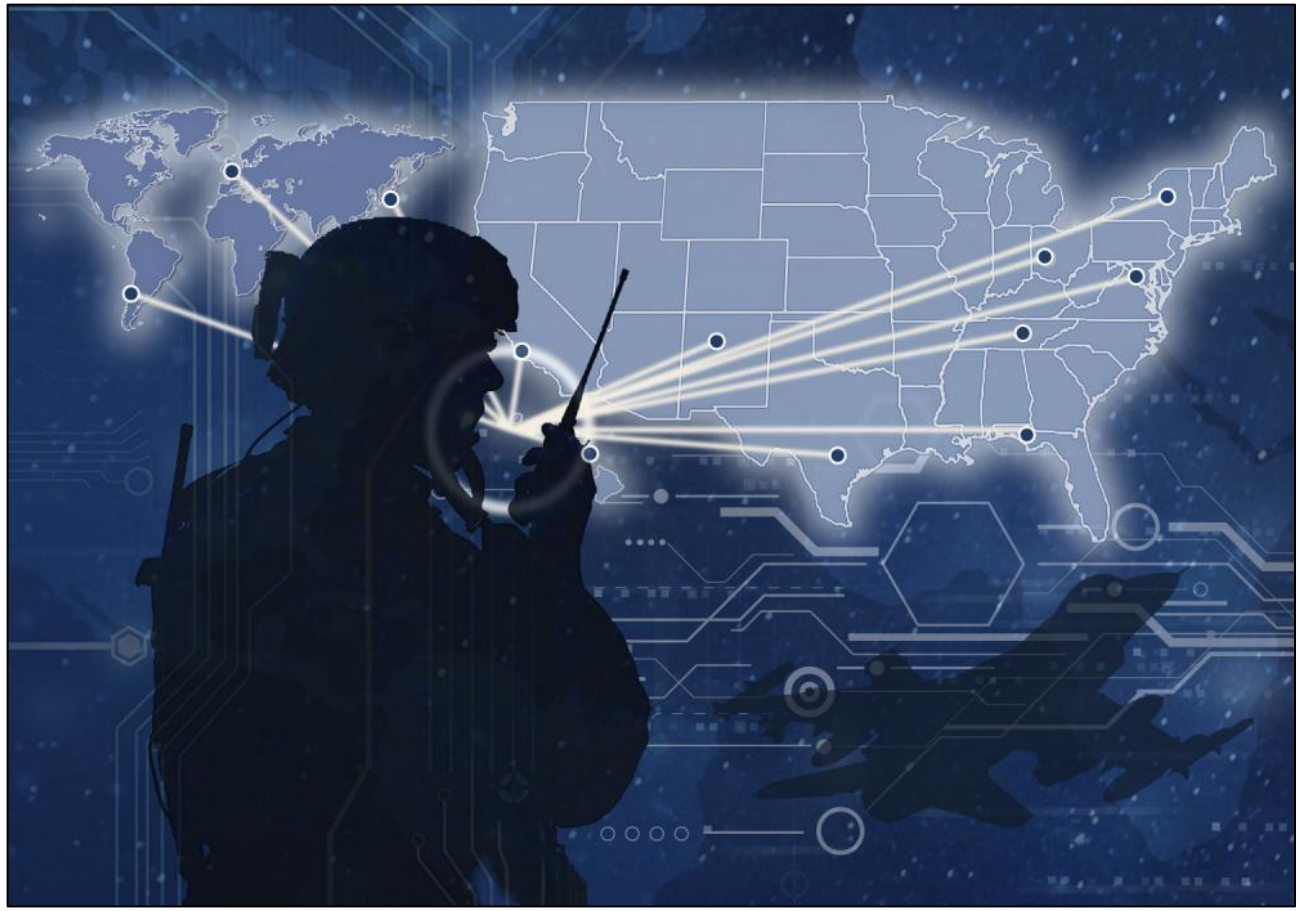
Addressing Effects (Expanded)

- **Identify constraints needed to address effects**
  - Constraints to avoid effects
  - Constraints to limit effects including duration
- **Enforce constraints**
- **Ensure enforcement (i.e., assurance of the constraint enforcement)**



What's Next

- **Articulate clearly protection as capability and functional driven**
- **Standardize practice with assurance deficit risk thinking**



Questions?

References

- Bider and Gould, editors, “The Coupling of Safety and Security.” https://doi.org/10.1007/978-3-030-47229-0
- National Aeronautics and Space Administration, “NASA Systems Engineering Handbook.” https://www.nasa.gov/connect/ebooks/nasa-systems-engineering-handbook
- Department of Defense, “Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs.” January 2017. https://www.dau.edu/tools/Lists/DAUTools/Attachments/140/RIO-Guide-January2017.pdf
- Department of Defense, “Technology and Program Protection to Maintain Technological Advantage.” 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf
- ISO, “ISO Guide 73:2009 – Risk Management Vocabulary.” 2009. https://www.iso.org/standard/44651.html
- “Systems Engineering Body of Knowledge.” 2022. https://www.sebokwiki.org/