REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
10/26/2020	Conference Briefing	

4. TITLE AND SUBTITLE
Concepts for an Approach to Weapon Systems Engineering

5a. CONTRACT NUMBER
W56KGU-18-D-0004

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Michael A McEvilley

5d. PROJECT NUMBER
0720D05ACA

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER
PRS-20-2837

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
United States Army (ACC-APG)

10. SPONSOR/MONITOR'S ACRONYM(S)
ACC-APG

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
Preprint to paper 23205 at NDIA 2020 Virtual Systems & Mission Engineering Conference, November 10, 12 – 13, 2020. NDIA.org/VirtualSME.

14. ABSTRACT

15. SUBJECT TERMS
Systems Engineering (General); Ordnance; tactical system design; weapon systems engineering; cyber-physical systems; protective system control; loss

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		23	Susan Carpenito
					19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646

Concepts for an Approach to Weapon Systems Engineering

Accounting for the Absence of Actionable Threat Data

Michael McEvilley
Principal Scientist

National Defense Industrial Association
23rd Annual Systems and Mission Engineering Conference
November 10-13, 2020

https://www.CTO.mil @DoDCTO

Topics

- Background
- Concepts overview
- Protective system control approach
- Next steps

Background

Basis of this Effort

- R&E Modernization Priority:
  - Advance Science and Technology (S&T) transition and systems security engineering, to include cyber, practice, and workforce competency
  - Deliver safe, secure, survivable, and resilient weapon systems in response to contested cyberspace concerns
- Informing elements:
  - DoDI 5000.83 “Technology and Program Protection To Maintain Technological Advantage”
  - Efforts in engineering community that comprise multidisciplinary approaches to advance security engineering practice
  - Cyber Resilient Weapon Systems (CRWS) Workshops
    - Means for the government, industrial, and academic elements of the weapon systems community to collaborate and solve problems

Maintain the Department's technological advantage and ensure alignment with the National Defense Strategy and R&E Modernization Priorities

Key Findings from Analysis to Achieve Synergy with System Safety

- Develop a comprehensive system security process that is informed by the system safety process
  - Adapt and apply safety approaches and methods to address the objectives of security
- Establish a “design for assurance” foundation
  - Substantiated confidence through the application of sound design principles and concepts
- Recognize the limits of certainty and transform those limits to risk
  - Insufficient confidence may translate to risk that must be identified, accepted, or addressed
  - Risk has individual and aggregate forms – both must be addressed to account for system risk
- Define an adverse effects (loss) basis for design
  - Controlling the potential for loss is the basis for safety and security engineering
  - Loss scenarios capture and relate the causal factor and state conditions that result in a loss
- Develop the security equivalent of the safety design order of precedence.
  - Design order of precedence optimizes the ROI for the reduction of susceptibility, hazard, and vulnerability

Reference: M. McEvilley, G. Vecellio, “Strategic Vision for Safety and Security in Weapon Systems Engineering”, MITRE Technical Report/MTR 180261, July 2018

Concepts Overview

Summary of Concepts

- Design Basis
  - Cyberspace and cyber-physical systems
  - Strategic and tactical perspectives
  - Loss protection assets, objectives, scenarios
- Design Strategy
  - Assurance as a risk driver
  - Design order of precedence
  - Protective system control

Cyberspace and Cyber-Physical Systems

- Cyberspace as an Operational Domain [1]
  - Cyberspace is a global domain within the information environment
  - Encompasses the interdependent networks of information technology infrastructures and resident data, telecommunications networks, computer systems, and embedded processors and controllers.
  - Interacts with the system types and operations that take place in the physical domains of air, land, maritime, and space.
- Cyber-Physical Systems [2]
  - The integration of computation, communication, actuators, sensors, and storage elements
  - Have inherent ability to monitor and control physical processes utilizing feedback loops such that physical processes affect computations and vice versa, with varying degrees of human intervention

[1] JP 3-12, Cyber Operations, 8 June 2018
[2] Edward A. Lee and Sanjit A. Seshia, Introduction to Embedded Systems: A Cyber-Physical Systems Approach, Second Edition, MIT Press, ISBN 978-0-262-53381-2, 2017)

Cyberspace and cyber-physical systems are different

Engineering in response to contested cyberspace requires addressing both

Strategic and Tactical System Design Perspectives

- Strategic Perspective for Design
  - Strategic security design approaches provide a basis to establish and maintain system capability and performance requirements while minimizing the extent of loss.
  - Strategic approaches provide a framing mechanism for the employment of tactics as part of an overall loss prevention strategy.
- Tactical Perspective on Controlling Loss
  - Tactical methods translate to component-level or lower (i.e., functions within a component) in the form of mechanisms or devices that serve as safeguards, countermeasures, and controls.
  - Tactics-oriented solutions are unable to account for system level problems that are reflected by emergence and side-effects of system function.
  - Tactics require a strategy for their optimum effectiveness. Systems engineering, through design trades and optimization, seeks a cost-effective balance between objectives, strategy, and the application of tactics.

Reference: William Young and Nancy Leveson, "Systems Thinking for Safety and Security", ACSAC'13, Dec. 9–13, 2013, New Orleans, Louisiana

Strategic and tactical perspectives are captured in the Design Order of Precedence

Asset Classes as the Loss Basis

- **System Capability Asset Class**
  - System capability is protected from loss if the system can deliver the capability at the specified level of performance
- **Human and Material Resource Asset Class**
  - Human resources are not harmed or killed
  - Material resources are not destroyed or unable to function as needed when needed
- **Technology Asset Class**
  - Technology is protected from loss if the technology is not exposed (e.g., read, copy, stolen) in an unauthorized manner, or reverse-engineered in an unauthorized manner
- **Data and Information Asset Class**
  - Protect data and information from loss due to unauthorized alteration, exfiltration, infiltration, to include destruction
    - Classified data and information protection against loss in the form of sources, means, and methods
    - Unclassified but sensitive data and information protection such as privacy data

System design must be cognizant of the differing protection needs and solutions associated with the 4 asset classes

Loss Control Objectives

Loss Objective	Elaboration

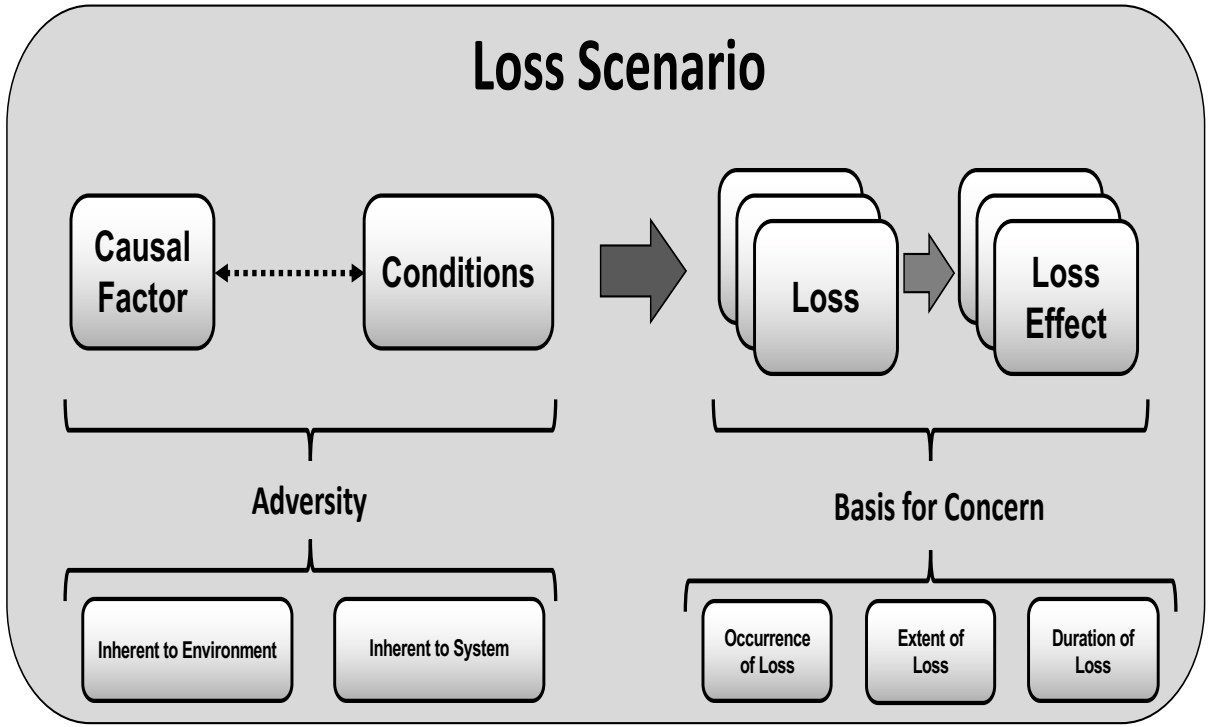
Prevent the loss from occurring	• This is the case where a loss is totally avoided. That is, despite the presence of adversity:
	  ○ The system continues to provide only the intended behavior and interactions, and produces only the intended outcomes
	  ○ The desired properties of the system and assets used by the system are retained
	  ○ The assets continue to exist
	• This may be achieved by preventing or removing the event(s) that would cause the loss, by preventing or removing the condition(s) that allows the loss to occur, or by not suffering an adverse effect despite the event(s) or condition(s).

Limit the extent of the loss	• This covers cases where a loss has occurred, and the extent of loss is to be limited.
	• The extent of loss can be limited in terms of any combination of the following:
	  ○ Limited dispersion (e.g., migration, propagation, spreading, ripple, domino, or cascading effects)
	  ○ Limited duration (e.g., milliseconds, minutes, hours, days)
	  ○ Limited capacity (e.g., diminished utility, delivery of function, service, or capability)
	  ○ Limited volume (e.g., bytes of data, information)
	• Loss recovery is one means of limiting loss. That is, the restoration of the asset, fully or partially, has the effect to limit dispersion, duration, capacity, or volume of the loss.

Loss control objectives define the target for engineering design to maximize protection effectiveness against capability and performance priorities and constraints

Loss Scenarios

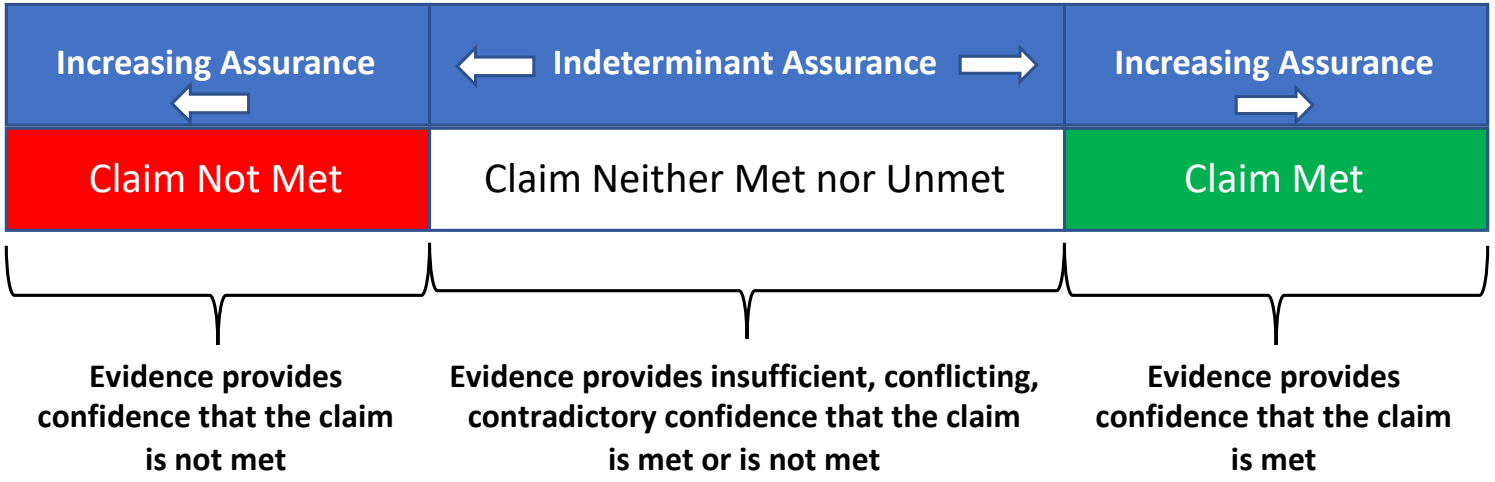
- Construct that captures and relates the constituent elements of adversity for a given loss
  - Provides a basis for analyses of loss
  - Informs analysis to determine response action and to assess the effectiveness of response action
  - Informs risk identification, assessment, and associated mitigation decisions



Loss scenarios enable development of modeling constructs for adversity and loss

Assurance Definition and Basis

Assurance: grounds for justified confidence that a claim has been or will be achieved (IEEE 15026-1:2019)



Assurance Basis

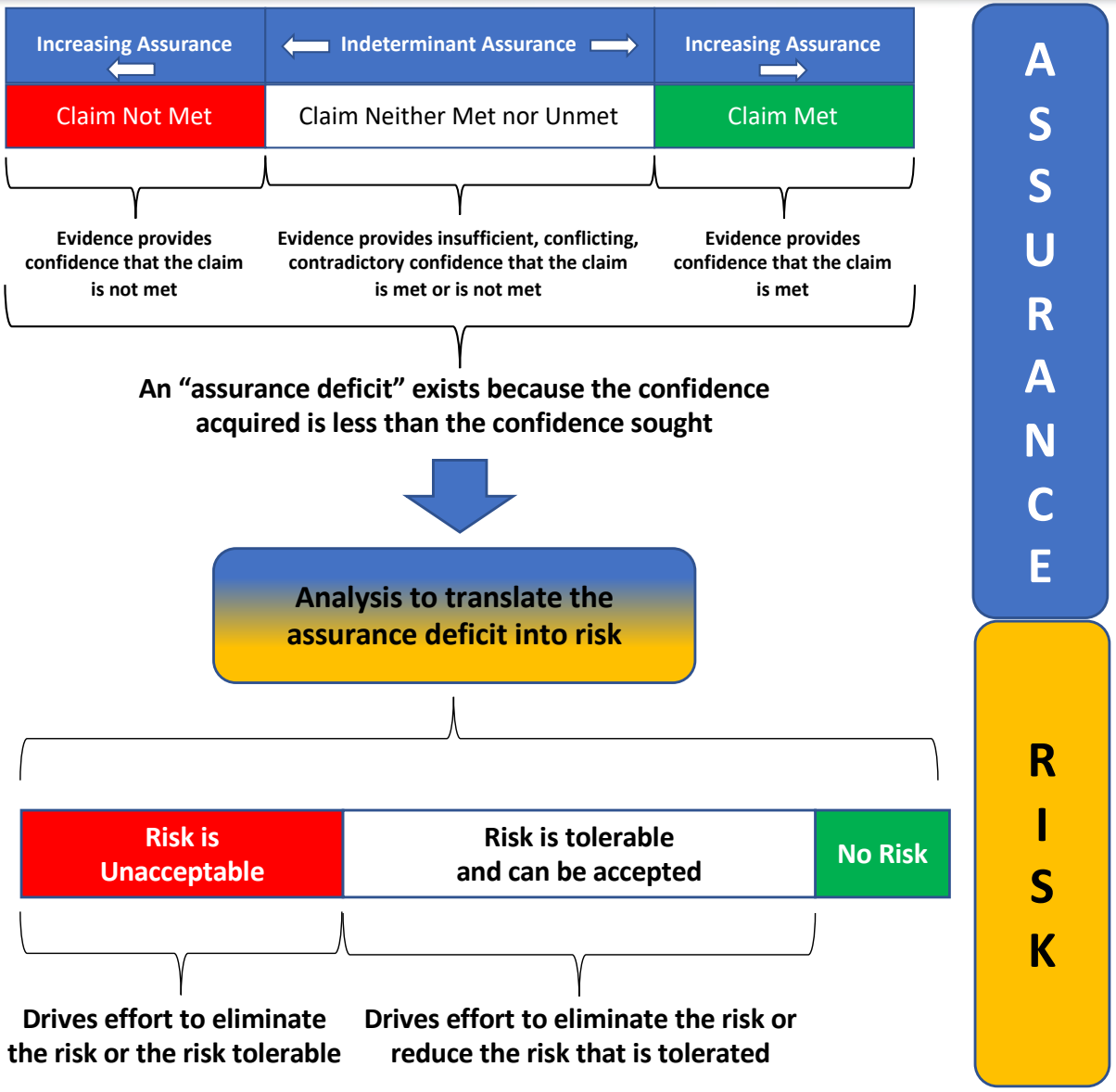
- **Explicit claims** - Claims must articulate precisely the properties the system is expected to exhibit and the assumptions about the system's environment in which the claim is contingent.
- **Evidence** - Concrete evidence must be present that substantiates the claims.
- **Expertise** - Expertise provides reasoned and informed judgements given the veracity of the evidence to support or substantiate the claims.

Source: National Academy of Sciences, "Software for Dependable Systems – Sufficient Evidence?", Committee on Certifiably Dependable Software Systems, 2007

Insufficient grounds for justified confidence is a driver of risk

Assurance and Risk

- Insufficient confidence is transformed into risk
  - Risk identification
  - Risk assessment
- Insufficient confidence may result from
  - Unknown and underappreciated threats, attacks, susceptibility, hazard, vulnerability



Design Order of Precedence

- **Design selection** to eliminate the inherent susceptibility, hazard, and vulnerability, thereby reducing the potential for loss
- **Design alteration** to reduce the potential, severity, or extent of loss caused by inherent susceptibility, hazard, or vulnerability
- **Employment of engineered features and devices** to control the effects of inherent susceptibility, hazard, and vulnerability
- **Provide situational awareness** mechanisms and accompanying procedures and training to enable personnel to deal with losses that occur

Adapted from MIL-STD-882E, DoD Standard Practice System Safety, 11 May 2012

Risk-informed design to reduce susceptibility, hazard, vulnerability

Differentiates the principles of secure system design and the control objective to limit the occurrence and extent of loss

Protective System Control

- Fusion of control, safety, and security concepts to establish a control system capability
- System control is comprised of the structure, features, and devices that collectively exercise control over a controlled process with the goals to
  - Enforces constraints on system behavior and outcomes
  - Provides for its own self-protection against targeted attack
  - Minimizes control function-induced emergent, erroneous, unsafe or non-secure control actions
  - Effectiveness is informed by but not dependent on the capability, means, and methods of an attacker
  - Ensure that only intended behavior and outcomes occur without experiencing an unacceptable loss
  - Not introduce loss scenarios that otherwise would not exist
- "Protective" system control requires inclusion of a generalization of the reference monitor concept of secure system design

Generalized Reference Monitor Concept

- The generalized reference monitor concept provides a uniform design assurance basis for any trustworthy system control or constraint-enforcing mechanism
- Two elements
  - Reference Monitor Concept (RMC) for design assurance for an access control reference validation mechanism:
    - The reference validation mechanism must be tamper-proof
    - The reference validation mechanism must always be invoked
    - The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured
  - NEAT extension to the RMC
    - Four necessary attributes of security protection mechanisms
    - **N**on-bypass-able, **E**valuate-able, **A**lways invoked, and **T**amperproof
- Successful achievement of these attributes will prevent interference of outside entities on a “controller”
  - A controller includes but is not limited to protection mechanisms

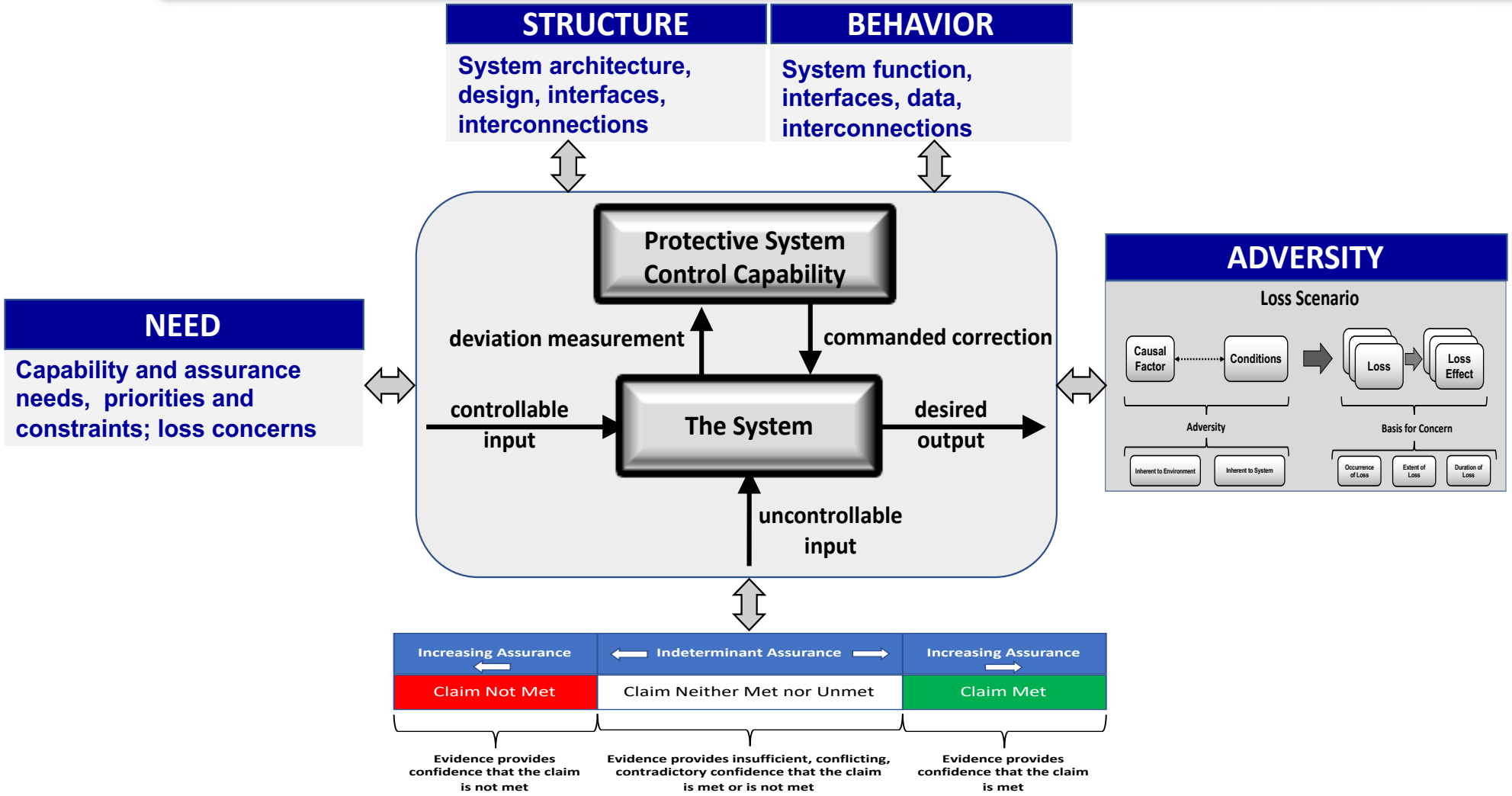
Protective System Control Approach

Protective System Control-Based Approach for Design

- A confidence-building, loss-driven/adverse-effects based approach
- Enforces constraints and exercises control to ensure predictable system behavior and outcomes that protects assets from intentional and unintentional adversity
- Differentiates between known and unknown or underappreciated technical understanding
  - Threat posed by an adversary
  - Attacks orchestrated and executed by an adversary
  - Environment and system inherent contributors to risk
    - Susceptibility, hazard, vulnerability
  - Assurance deficit as a contributor to risk

"Systems [must] behave with predictability and proportionality"
– General Michael Hayden, Former National Security Agency (NSA) and Central Intelligence Agency (CIA) Director

Comprehensive Concept for Design



Underlying foundation of engineering design, trustworthiness, and loss control design principles

Next Steps

Next Steps

- Formalize the concept of protective system control
- Transform the other concepts into an approach based on protective system control
- Expand approach to include results of ongoing efforts
  - Maturation of design principles and associated patterns
  - Development of patterns for resilience and security requirements
- Derive content for inclusion in the CRWSBok (Cyber Resilient Weapon Systems Body of Knowledge)