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

Design Principles for 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-20-2768

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 23204 at NDIA 2020 Virtual Systems & Mission Engineering Conference, November 10, 12 – 13, 2020.

14. ABSTRACT

15. SUBJECT TERMS

Systems Engineering Standards; Ordnance; tactical system design; standardization; weapon systems engineering; cyber-physical systems; protective system control; loss control

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

Design Principles for Weapon Systems Engineering

Michael McEvilley
Principal Scientist

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

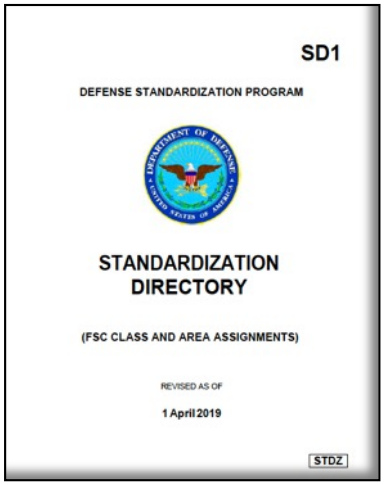
https://www.CTO.mil *@DoDCTO*

Topics

- Background of the study
- Approach to develop the principles
- Overview of the 3 principle classes
- Key finding for future work
- Next steps

Basis of this Effort

- OUSD(R&E) Goals:
  - 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


SD1

DEFENSE STANDARDIZATION PROGRAM

STANDARDIZATION DIRECTORY

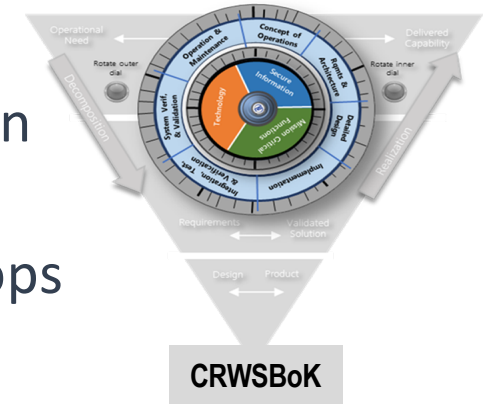
(FSC CLASS AND AREA ASSIGNMENTS)

REVISED AS OF

1 April 2019

STDZ

- Informing elements
  - DoDI 5000.83 “Technology and Program Protection To Maintain Technological Advantage”
  - Cyber Resilient Weapon Systems (CRWS) Workshops



CRWSBoK

Principled design content is the basis for standardization and the foundation for a body of knowledge

Key Findings of CRWS Workshop Series

- Recognition of value derived from safety practice
  - Ensure alignment with system safety
- "Do systems engineering right"
  - Employ an engineering and development model
  - Proper application of secure design principles, concepts, patterns, and techniques to weapon systems
- Weapon system characteristics
  - Real-time, embedded function, control systems, and interconnected information systems
  - Operate in the physical domains of air, land, maritime, and space, and the virtual domain of cyberspace
  - Adversarial threats span the domains whereby causal events in one may result in effects in the other
- Better recognition of the limits of certainty
  - Software behavior
  - Threat behavior (adversarial and non-adversarial)
  - Uncertainty as a source of risk

CRWS 8 Design Focus

- Collection of 37 principles, concepts, and techniques
  - Curated from engineering, computational science, safety, security, loss prevention, and resilience communities
  - Focus on their relevance and value to system design independent of community-specific objectives, assumptions, and priorities
  - Selected from ~70 candidates
- Relevant to system objectives for resilience, security, and survivability
  - System structure and architecture
  - System intrinsic capability and behavior
  - Strategies and approaches for trustworthiness

CRWS 8 Design Focus Findings

- Need for uniform vernacular
  - Language and terms varied
  - Too specialty oriented in some cases
- Need for structure, association, grouping
  - Recommendations to separate types, means, and ends
- Need for clarity and value
  - Greater emphasis on design value to achieve objectives
  - Less emphasis on “Engineering 101/Hygiene”

Approach for Standardization

- Establish a foundation
  - Not an authoritative, exhaustive, or complete
- Develop lexicon/vernacular/taxonomy that suffices for use in engineering analytical activities.
  - Definitions
  - Formal syntax and semantics
- Build Consensus
  - Foundation enables consensus-building and continuous improvement
  - Vetted content will comprise standardization within the SCRE Defense Standardization Area, and content to be incorporated in the associated engineering body of knowledge (BoK)
- Extend the knowledge over time
  - Improved and additional principles
  - Patterns for requirements, design, loss scenarios, and adversity scenarios
  - Support for modeling, formal specification, and formal verification

Establish a rigorous basis for assurance

Approach to Transform the Design Materials into Principles

- Prioritize the objective to protect assets from loss
  - Focus on what loss is and what it means
- Enable balance in addressing loss
  - What is possible vs what is likely
- Accept limits of certainty regarding "how" the loss occurs
  - i.e., the adversity-to-loss relationship
- Differentiate where to emphasize on cause vs effect
  - Adversity-dependent emphasis when there is sufficient knowledge of how the loss can occur
  - Adversity-independent emphasis when there is insufficient knowledge or no knowledge of how the loss can occur
- Employ diverse sources dating back decades
  - "Over the horizon view" to ensure we capture the essential works that may not be defined or described using today's terminology

Scoping Considerations

- Weapon system oriented
  - Defined and discussed relative to purpose and function of weapon systems
- Support for trade space options to achieve objectives
  - Multiple approaches and solutions to a given problem
- Requires judgement for proper application
  - Avoid prescriptive statements
    - Not a “set of rules to follow”
    - No order or sequence of application
  - May be conflicting or in contradiction with each other

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
  - Generally, the capability and performance is a function of (a) the role of the system to support mission objectives and (b) the nature of the system (e.g., aircraft, missile, surface ship, tactical ground vehicle, submarine, sensor, unmanned vehicle)
- **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 in an unauthorized manner (read/copy/stolen), or reverse-engineered in an unauthorized manner
  - Focus of anti-tamper protection and is an extension of the protection of means and methods
- **Data and Information Asset Class**
  - Protect data and information from loss due to unauthorized alteration, exfiltration, infiltration, to include destruction
  - Data and information protection is historical basis for security
    - 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

Loss Control Objectives

Loss Control Objective	Description	Elaboration

Loss Prevention	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).
		• Terms such as *avoid, prevent, remove, eliminate, harden, tolerate, withstand,* and *continue* fall into this objective when the loss does not occur despite the system being subjected to adversity.

Loss Limitation	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)
		• Decisions to limit the extent of loss may require prioritizing what constitutes acceptable loss across a set of losses, whereby the goal to limit the loss for one asset requires accepting a loss for some other asset.
		• The extreme case of loss limitation is to avoid destruction of the asset.
		• Terms such as tolerate, withstand, remove, continue, constrain, stop/halt, and restart fall into this category for the case where the loss occurs, and the system is able to, or enables the ability to, limit the effect of the loss.
		• 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.
		  ○ This is the case where action is taken by the system or where action is enabled by the system to recover (allow the recovery of) some or all of its ability to function (behave, interact, produce outcomes) and to recover assets used by the system (e.g. re-imaging, reloading or recreating information and data, including software in the system).
		  ○ Terms such as *recover, restore, reconstitute, reconfigure*, and *restart* fall into this category.

Principle Categories

- Engineering design principles
- Trustworthiness design principles
- Loss control design principles

Each principle has the following structure

- Title
- Description
  - One or two sentences
- Elaboration
  - Explain value, facilitate proper interpretation, provide application considerations
- References
  - Informing sources or source for additional information

Engineering Design Principles and Tenets

Manage complexity and aid in understanding the engineered system in depth

Title	Description
Clear Representation	The abstractions used to characterize the system for systems engineering purposes should be simple, well-defined, accurate, precise, necessary, and sufficient.
Composition Principles	System complexity should be managed through a structured decomposition of the system into cohesive constituent elements (modularity) and composing the constituent elements in accordance with relational rules to deliver required capability (layering).
Reduced Complexity	The system design should be as simple as practicable given the inherent complexity that the design represents.

Trustworthiness Design Principles and Tenets

Facilitate design trade space decisions that are necessary given the impracticality of every system element having the desired trustworthiness

Title	Description
Commensurate Rigor	The rigor associated with the conduct of an engineering activity should provide the confidence required to address the most significant adverse effect that can occur.
Commensurate Trustworthiness	An element must be trustworthy to a level commensurate with the most significant adverse effect that results from a failure of that element.
Compositional Trustworthiness	The design for the system should be trustworthy for each aggregate composition of interacting elements.
Generalized Reference Monitor Concept	An abstract model of the necessary and sufficient properties for the design of any system mechanism that provides a control function to enforce constraints.
Hierarchical Protection	An element need not be protected from more trustworthy elements.
Minimized Trusted Elements	A system should have as few trusted elements as practicable.
Self-Reliant Trustworthiness	The trustworthiness of an element should be achieved with minimal dependence on other elements.
Substantiated Trustworthiness	System trustworthiness judgements must be based on evidence demonstrating that the criteria for trustworthiness has been achieved.

Loss Control
Design Principles and Tenets (1/2)

Loss control seeks to limit the extent to which the system is manipulated, attacked, misused, or abused in a manner that intentionally or unintentionally produces a loss

Title	Description
Anomaly Detection	Any salient anomaly in the system or in its environment is detected in a timely manner that enables effective response action.
Commensurate Protection	The strength and type of protection provided to an element must be commensurate with the most significant adverse effect that results from a failure of that element.
Commensurate Response	The design strategy for the system should seek to match the aggressiveness of an engineered response action to the needed immediacy in controlling the effects of each loss scenario.
Continuous Protection	The protection provided for an element must be effective and uninterrupted for the entirety of the time that the protection is required.
Defense-in-depth	Loss is prevented or minimized by the employment of multiple coordinated mechanisms.
Distributed Privilege	Multiple authorized entities must act in a coordinated manner before an operation on the system is allowed to occur.
Diversity (Dynamicity)	The design delivers the required capability through the incorporation of structural, behavioral, or data flow variation.
Domain Separation	Domains with distinct protection needs should be physically or logically separated from other domains.

Loss Control
Design Principles and Tenets (2/2)

Loss control seeks to limit the extent to which the system is manipulated, attacked, misused, or abused in a manner that intentionally or unintentionally produces a loss

Title	Description
Least Persistence	System elements and resources should be available, accessible, and able to fulfill their design intent only for the time they are needed to perform a system operation.
Least Privilege	Each element should be allocated privileges that are necessary to accomplish its specified functions, but no more.
Least Sharing	System resources, including mechanisms, should be shared among system elements only when necessary, and among as few system elements as possible.
Loss Margins	The system remains in a state space such that the loss scenarios are sufficiently distanced below the threshold at which loss occurs.
Mediated Access	All attempts to perform operations on system elements are mediated.
Protective Defaults	The default configuration of the system provides maximum protection effectiveness.
Protective Failure	A failure of a system element should not result in an unacceptable loss, nor invoke another loss scenario.
Protective Recovery	The recovery of a system function or other asset should not result in, nor lead to, unacceptable loss.
Redundancy	The design delivers the required capability by the replication of functions or elements.

Key Finding
Need for Protective System Control

- Protective system control
  - What:
    - The fusion of multidisciplinary methods to provide a system control capability
  - Properties:
    - Achieves only the intended system behaviors (ideal) despite all forms of intentional and unintentional adversity
    - Provides for its own self-protection
  - Basis:
    - Systems thinking, control systems thinking, safety thinking, secure system design thinking
    - Design principles targeted to the loss control objectives

"Systems [must] behave with predictability and proportionality"
General Michael Hayden, Former NSA and CIA Director

Next Steps

- Capture the design principles in the CRWSBok
- Use the design principles to support Secure Cyber Resilient Engineering (SCRE) standardization
- Revisit design principles and associated patterns at CRWS 10
- Develop the concept of Protective System Control for weapon systems

Questions