A Loss-Driven Approach to Systems Analysis

Ms. Melinda Reed
Strategic Technology Protection & Exploitation
Office of the Under Secretary of Defense (Research & Engineering)
Mr. Michael McEvilley
MITRE Corporation

22nd Annual NDIA Systems and Mission Engineering Conference
Tampa, FL | October 24, 2019

Overview

- Loss-driven basis for Systems Engineering
- Systems analysis approach to address the potential for loss

Loss-Driven Systems Engineering

- **Purpose of systems engineering is to "deliver capability to the warfighter"**
  - Defense Acquisition Guide (DAG) Chapter 3
- **Loss associated with the system has effects**
  - Effects span the life cycle of the system
  - Capability needs – which include mission objectives – are not the sole basis to define loss
    - Collateral damage, life, means and methods, etc.
- **Loss-driven SE addresses the potential for loss associated with the "delivery of capability"**
  - The "flip side" of capability-driven SE
  - Applies to entire system, system of systems (SoS), acquirer, and supplier life cycles

Systems Engineering

Capability ➡ **Meet performance expectations: Capability-driven**

Loss ➡ **Meet acceptable loss expectations: Loss-driven**

Engineering to Address the Potential for Loss

- **Fundamental challenge facing security professionals is preventing losses**
  - "**Systems Thinking for Safety and Security**" by Col William Young (USAF) and Nancy Leveson (MIT)
- **Scope of loss includes:**
  - Death, injury, or occupational illness
  - Damage to or loss of equipment or property
  - Damage to or loss of data or information
  - Damage to or loss of capability, function, or process
  - Damage to the environment
- **Loss concerns are the basis for security activities and judgments**
  - … and safety, survivability, resilience, …
  - … and other quality properties of the system

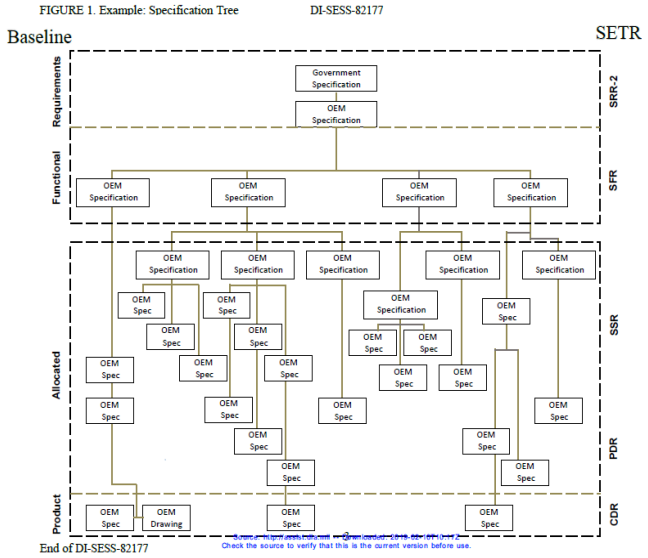
The Meaning of "Protect Against Loss"

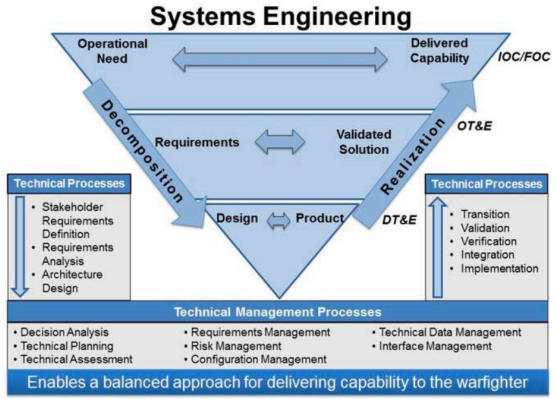
- **Protecting against loss and the associated effects is an objective**
  - Prevent the occurrence of loss or the associated effect
  - Limit the loss or associated effect
    - Physical, geographic extent of loss
    - Temporal extent of loss
    - Utility extent of loss
  - Recover from loss or the associated effect
- **Protecting against loss focuses on effect – in consideration of all causes and conditions**
  - Attacks, misuse, abuse
  - Faults, errors, failures
  - Natural, man-made
  - Human, machine, environment
  - Defects, flaws
  - Exposure, hazards, vulnerabilities
- **Protecting against loss encompasses the objectives driven by the domain referred to as cyberspace**
  - Cyberspace is the information domain that exists in context of the physical domains of air, land, maritime, and space
  - Addressing loss enabled/induced by cyberspace encompasses the "cyber triad" of cyber security, cyber survivability, and cyber resilience

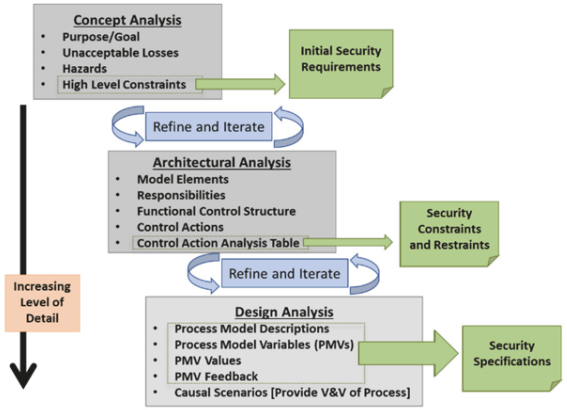
Understanding how loss occurs is necessary to protect against loss

Strategy to Understand Loss: Systems Analysis of Loss

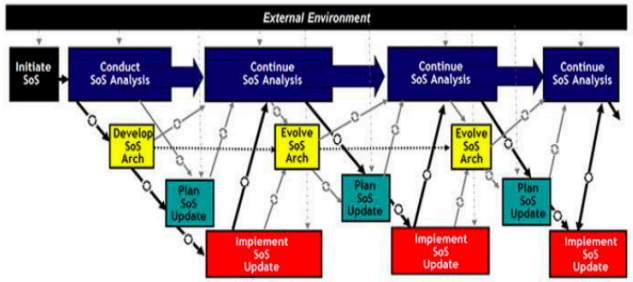
Analysis achieves system-level technical understanding of the dynamics of security-relevant loss potential; independent of specific model, framework, application, or purpose

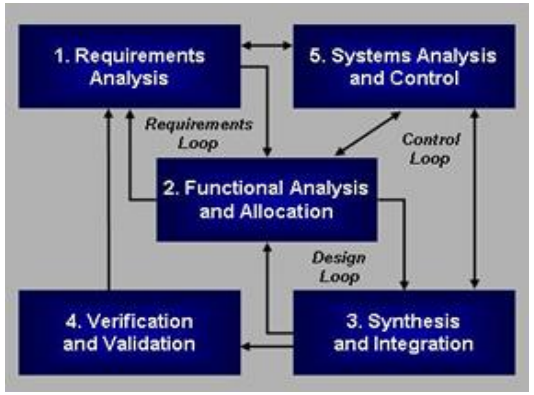




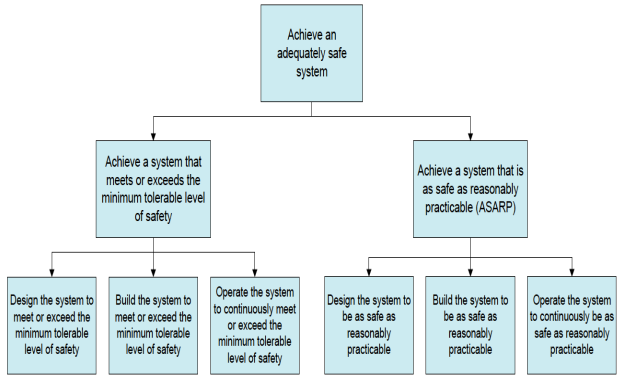


Source: "A Systems Security Approach for Requirements Analysis of Complex Cyber-Physical Systems", Span, Mailloux, Grimaila, Young





Source: The Boeing Company



Source: NASA

The need for systems analysis is everywhere

Loss-Driven Systems Analysis

- **Is about the:**
  - System as defined by IEEE 15288
    - A combination of interacting elements organized to achieve one or more stated purposes
    - Emergence and side effects at component level, function level, end-to-end level
  - Types of loss arising from development or use of the system
    - The meaning of loss varies
- **Is not**
  - Mission thread analysis
  - Threat assessment, vulnerability assessment, or risk assessment
  - Limited to cyberspace

The Cyber-Physical Aspect of Systems

- **A cyber-physical system (CPS) is an integration of computation with physical processes**
  - Emerged in 2006, coined by Helen Gill at the National Science Foundation (NSF)
  - Requires understanding the interaction between physical components and the computational components.
  - Design and analysis requires understanding the joint dynamics of computers, software, networks, and physical processes.
  - Has roots that are older and deeper than the term "cyberspace"
- **"Cybernetics" is the root for both cyberspace and cyber-physical systems**
  - "Cybernetics" was coined by Norbert Wiener (Wiener, 1948), mathematician with huge impact on the development of control systems theory
  - Cybernetics is derived from the Greek *kybernetes*, meaning helmsman, governor, pilot, or rudder
  - During World War II, Wiener pioneered technology for the automatic aiming and firing of anti-aircraft guns.
  - The control logic is effectively a computation, and therefore cybernetics is the conjunction of physical processes, computation, and communication.
  - Computation is achieved by analog and digital processes, and by hardware or software

Systems analysis has to address the cybernetic properties of the systems

Source: Lee and Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, LeeSeshia.org, 2011. (https://ptolemy.berkeley.edu/projects/cps/Cyber-Physical_Systems.html)

Purpose of Systems Analysis*

- **Provide a rigorous basis of data and information for technical understanding to aid decision-making across the life-cycle**
- **Provide confidence in system requirements, architecture, design**
  - The confidence achieved is a function of the formality and rigor applied in the conduct of the analysis, the data that informs the analysis, and the tools used to support the analysis.
  - The formality and rigor should be commensurate with the criticality of the data/information need, product supported, decision to be made, the quality and amount of data/information available.

**15288 mentions the coupling between the Systems Analysis and Decision Processes; DoD System Engineering integrates the 15288 notion of Systems Analysis into the Decision Analysis Process*

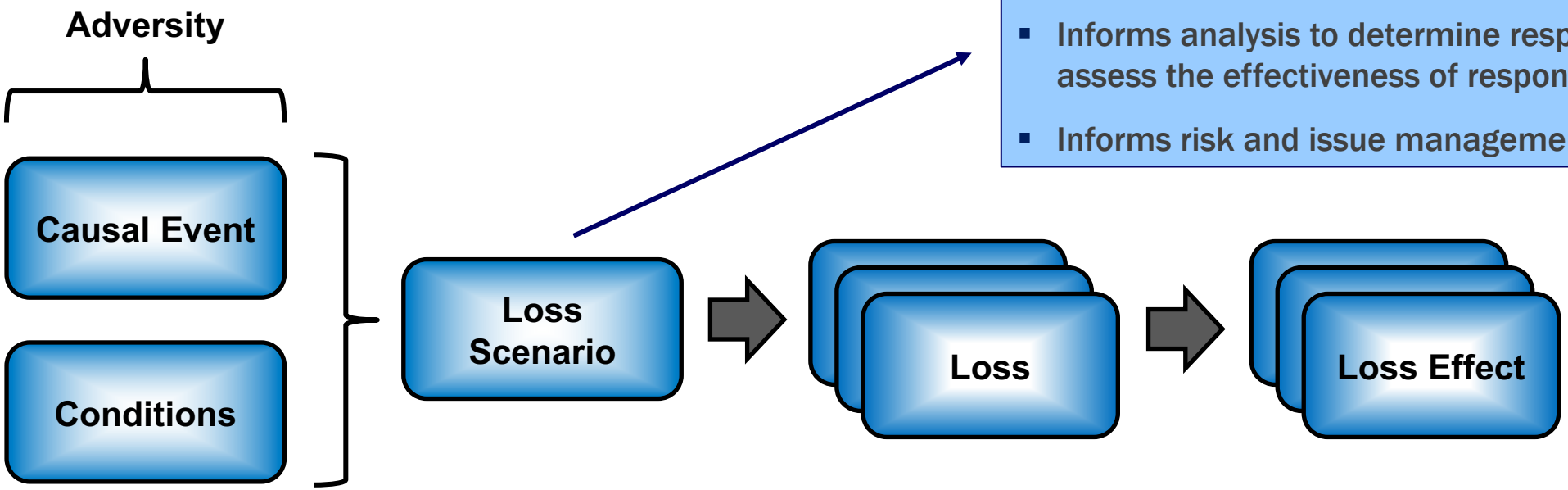
Injecting Potential for Loss into Systems Analysis*

- **Provide a rigorous basis of data and information for technical understanding of the subtleties and nuances associated with the potential for loss to aid decision-making across the life cycle**
- **Provide confidence in how well loss considerations are captured in system requirements, architecture, design**
  - The confidence achieved is a function of the formality and rigor applied in the conduct of the analysis, the data that informs the analysis, and the tools used to support the analysis.
  - The formality and rigor should be commensurate with the criticality of the effect of loss, the data/information need, product supported, decision to be made, the quality and amount of data/information available.

**15288 mentions the coupling between the Systems Analysis and Decision Processes; DoD System Engineering integrates the 15288 notion of Systems Analysis into the Decision Analysis Process*

Loss Scenario – Basis of Loss Analysis

- Describe the adversity in terms of its constituent causal event and condition elements and relationships
- Correlates adversity to specific losses and loss effects
- Informs analysis to determine response action and to assess the effectiveness of response action
- Informs risk and issue management activity



Systems Engineering

Optimize system design for the response to loss scenarios while meeting performance measures in accordance with stakeholder requirements and risk and issue decisions

Understanding how loss occurs is necessary to protect against loss

Loss-Driven Systems Analysis Key Focus Areas

NEED

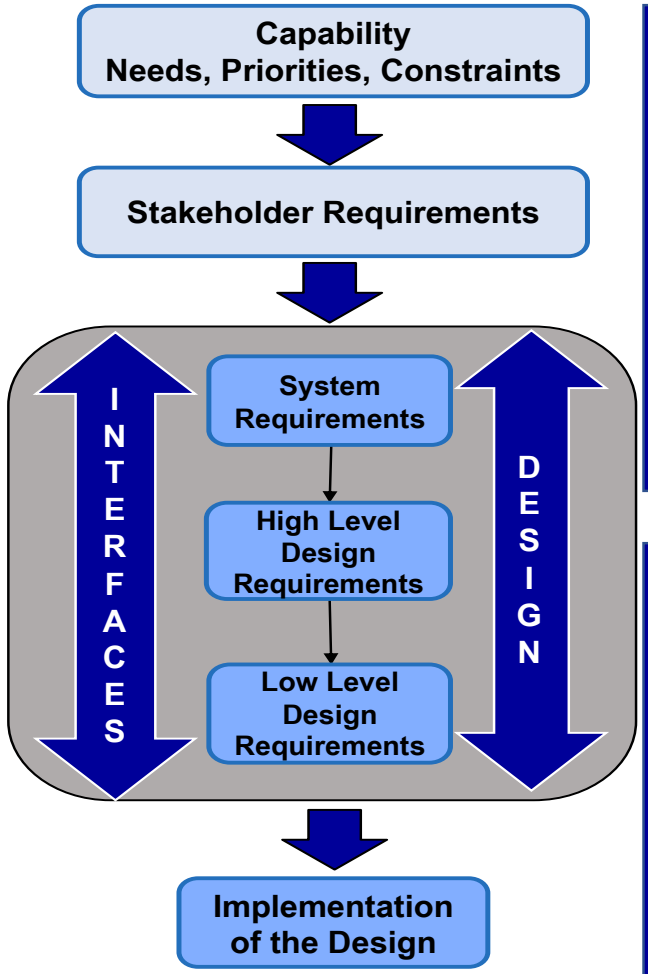
Capability needs, loss concerns, acceptance

- Mission
- System
- Regulatory, statutory, certification, policy
- Assurance

STRUCTURE

System architecture, design, interfaces, interconnections

- Exposure, hazards, vulnerabilities
- Critical functions
  - Mission
  - System
  - Security
  - Safety



ADVERSITY

Loss scenarios

- Causal factors
  - Attack, subversion
  - Error, fault, failure
  - Abuse, misuse
- Conditions
  - Exposure, hazard, vulnerability
- Adversarial threat informed
  - Threat data-dependent
  - Threat data-independent

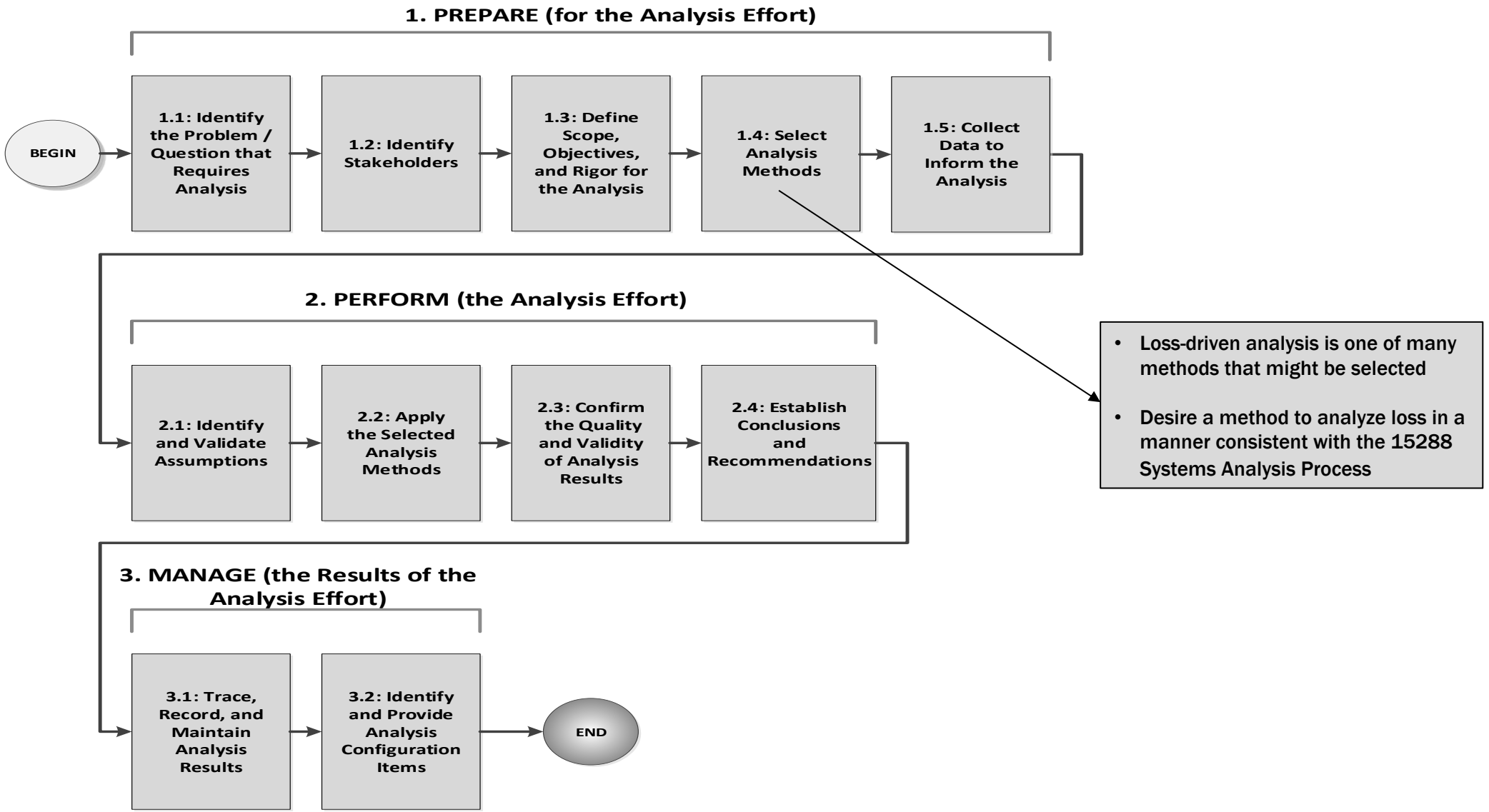
BEHAVIOR

System function, interfaces, data, interconnections

- Functional, data, control flow interactions
- Interactions not anticipated by the system requirements
- Exposure, hazards, vulnerabilities

Applied with rigor necessary to achieve the targeted level of confidence

IEEE 15288 Systems Analysis Process Activity Overview



Method for Analysis of Potential for Loss

(adheres to the structure of the IEEE 15288 Systems Analysis Process)

Prepare

- **Determine the criteria to conduct the loss analysis**
  - Determine the purpose of the analysis
  - Determine the data that is to be produced by the analysis
  - Identity stakeholders
  - Determine system scope, context, and rigor for the analysis
  - Determine the analysis acceptance criteria
- **Collect data to inform the loss analysis**
  - Collect data that describes the system function, functional elements, the system context, and the environment context
  - Collect data that describes the assets of concern, their role in the system, their significance, their priority, and the loss concern
  - Collect data that describes the adversity of interest
  - Collect data that describes the system response to adversity

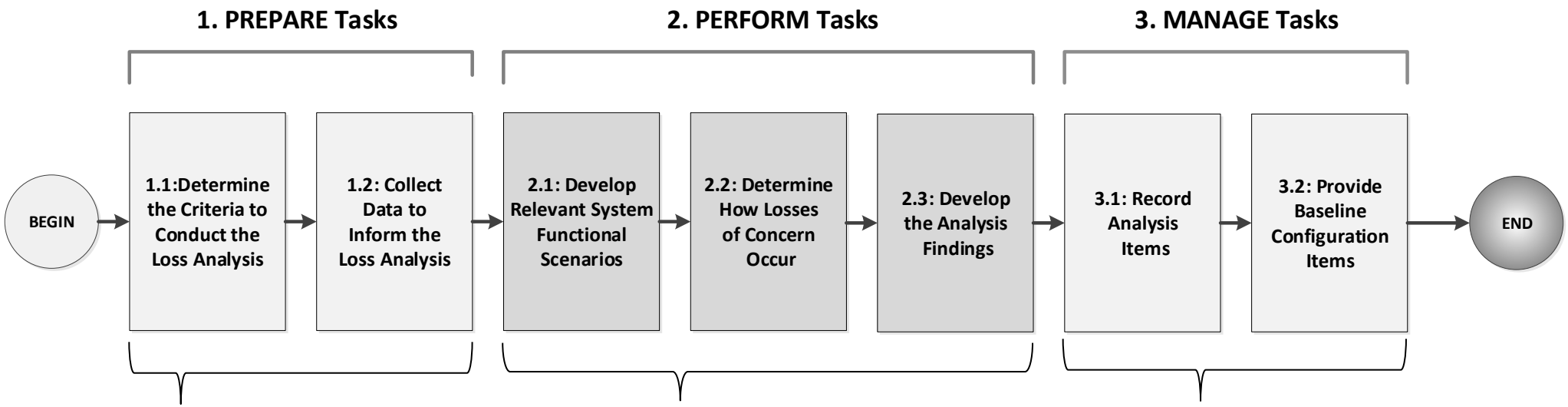
Perform

- **Develop relevant system functional scenarios**
  - Model the system structure
  - Model the system behavior
  - Model the control structure
  - Model the control behavior
  - Model data flows
- **Determine how losses of concern occur**
  - Develop causal scenarios
  - Categorize the losses associated with the causal scenarios
  - Explain how categorized losses occur
- **Develop the analysis findings**
  - Confirm the quality and validity of analysis findings
  - Record findings

Manage

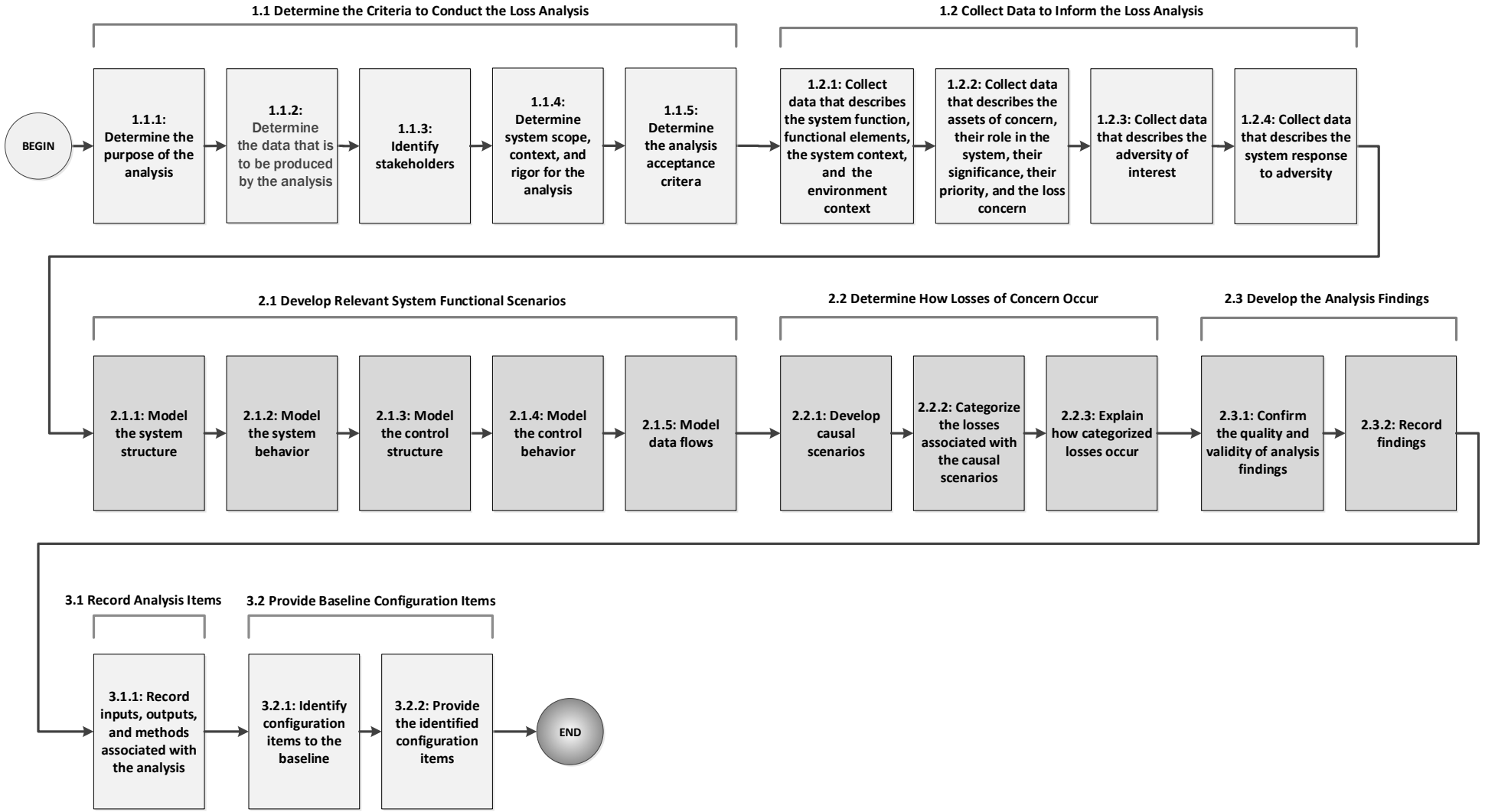
- **Record analysis items**
  - Record inputs, outputs, and methods associated with the analysis
- **Provide baseline configuration items**
  - Identify configuration items for the baseline
  - Provide the identified configuration items

Method for Analysis of Potential Loss High-Level Activity and Task Flow



- **IEEE 15288 Prepare**
  - Identify the problem or question that requires analysis
  - Identity stakeholders
  - Define scope, objectives, and rigor for the analysis
  - Select analysis methods
  - Collect data to inform the analysis
- **IEEE 15288 Perform**
  - Identify and validate assumptions
  - Apply the selected analysis methods
  - Confirm the quality and validity of analysis results
  - Establish conclusions and recommendations
- **IEEE 15288 Manage**
  - Trace, record and maintain analysis results
  - Identify and provide analysis configuration items

Method for Analysis of Potential Loss Detailed Task and Sub-Task Flow



(EXAMPLE OF TEMPLATE UNDER DEVELOPMENT)

PREPARE Activity: Determine the criteria to conduct the loss analysis

Purpose	Establish the reason to conduct the loss analysis, the criteria that determines how the analysis is conducted, and the basis to determine acceptance of analysis results
Outcomes	• Loss analysis needs are identified • Loss analysis success criteria are identified • Loss analysis scope and context is identified
Task Summary	**Elaboration**
• Determine the purpose of the analysis	• The purpose of the analysis is reflected in the problem to solve, the question to answer, the technical understanding that is sought, or the decision to be made.
• Determine the data that is to be produced by the analysis	• The data produced by the analysis directly supports the purpose of the analysis. The data may be produced solely by the loss analysis or be produced in combination with the results of other analysis. Recommendations informed by the data may also be provided.
• Identity stakeholders of the analysis	• The stakeholders of the analysis make judgements based on the results provided by the analysis. Successful completion of the analysis is dependent on meeting the expectations of all stakeholders. These stakeholders may have competing or conflicting needs associated with the purpose and success criteria of the analysis.
• Determine system scope, context, and rigor for the analysis	• Scope, context, and rigor includes: ▪ System architecture, function, functional elements ▪ System states, modes, and transitions ▪ Environment context ▪ Assets of interest, their priority of importance to stakeholders, the asset loss concerns ▪ Nature and type of loss to examine ▪ Specific adversity of interest ▪ System response to adversity ▪ Formality, thoroughness, accuracy, precision for the approach, methods, tools and outcomes of the analysis.
• Determine the analysis acceptance criteria	• Acceptance criteria is used to determine that the analysis is sufficiently complete and comprehensive with respect to the intended goals, validated assumptions, and constraints imposed

Informing Sources

- IEEE 15288 Systems Analysis Process
- DAG Chapter 3 Decision Analysis Process
- DoD System Safety (MIL-STD-882E)
- NASA System Safety, Systems Engineering, Risk-Informed Decision Making
- Systems Theoretic Process Analysis (STPA) and its security extension (STPA-Sec)
- Secure Design Principles

Summary

- A loss-driven approach to system analysis is proposed as a method to achieve technical understanding of the subtleties and nuances of loss
- The method is "specialty independent" to have application within and across all loss-driven engineering specialties
  - Safety, security, survivability, resilience, reliability, availability, maintainability, etc.
- Future "Pathfinder" sessions are planned
  - CRWS 8, February 2020
  - Exploring other opportunities

For Additional Information

Ms. Melinda Reed

Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E))

571.372.6562 | melinda.k.reed4.civ@mail.mil

Mr. Michael McEvilley

Contractor Support Team, MITRE Corporation

703.472.5409 | mcevilley@mitre.org

https://www.cto.mil

Questions?

Follow us @DoDCTO