Approved for Public Release; Distribution Unlimited. 16-3797

Putting the "Systems" in Security Engineering

An Overview of NIST 800-160

Systems Security Engineering

Considerations for a multidisciplinary approach for the engineering of trustworthy secure systems

NDIA 19th Annual Systems Engineering Conference
October 24, 2016
Springfield, VA.

Michael McEvilley
Max Allway
Alvi Lim

The MITRE Corporation
Systems Engineering Technical Center
mcevilley@mitre.org
703.983.5951

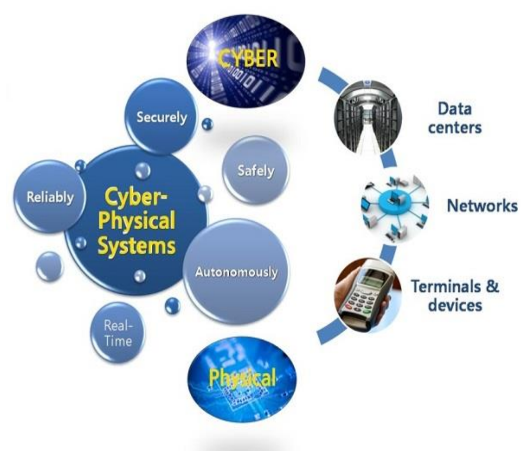
Agenda

- **Trustworthy Secure System Challenges**
- **Seven Key "Systems" Security Concepts**
  - Security, Secure System, Adequately Secure System
  - Assets, Loss, Context, Consequences
  - Predominate Views of System Security
  - Differentiating Security Protection and System Security
  - System Security and Failure
  - Secure Modes, States, and Transitions
  - System Security Trustworthiness
- **Systems Security Engineering in a Nutshell**
- **NIST SP800-160 Way Forward**

MITRE

Trustworthy Secure System Challenges

- **Systems are increasingly complex**
  - Dynamicity
    - Interactions, behaviors
    - Composition
  - Uncertainty
  - Emergence
- **Security is emergent**
  - A holistic system property
- **Failures are multifaceted**
  - Encompassing both unforced and forced forms
- **Interactions and behaviors**
  - Within and between the engineering team and stakeholders



Multidisciplinary Challenges Require Multidisciplinary Solutions

MITRE

What is System Security?

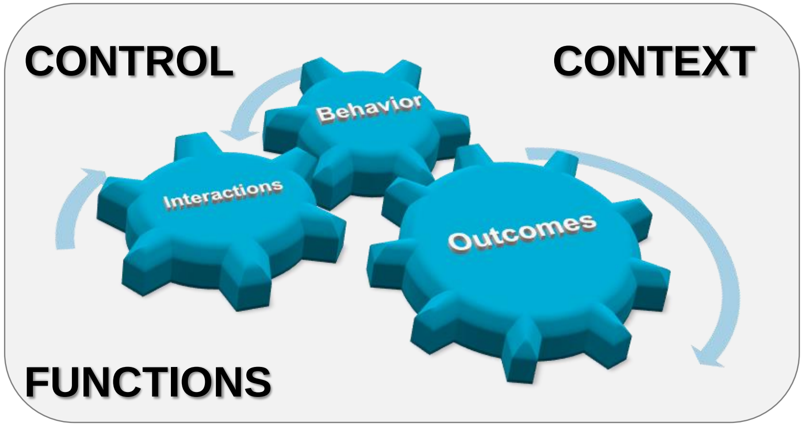
- **Prevailing definitions too narrowly-scoped**
  - Data and information, information technology, information systems
  - Associated properties of confidentiality, integrity, availability

- **No definition sufficed for the broad definition of "system"**
  - As used by IEEE and INCOSE
  - Sufficient to address the entirety of today's inherently complex systems

In Search Of … System Security Essentials

Behavior, Control, Loss, Context

- **Behavior, interactions, outcomes**
  - What the system does and does not do
- **Control objective to address asset loss**
  - Prevent, minimize, constrain, and limit the extent of asset loss and adverse consequences
- **Context-driven views**
  - Rarely is security a context of itself



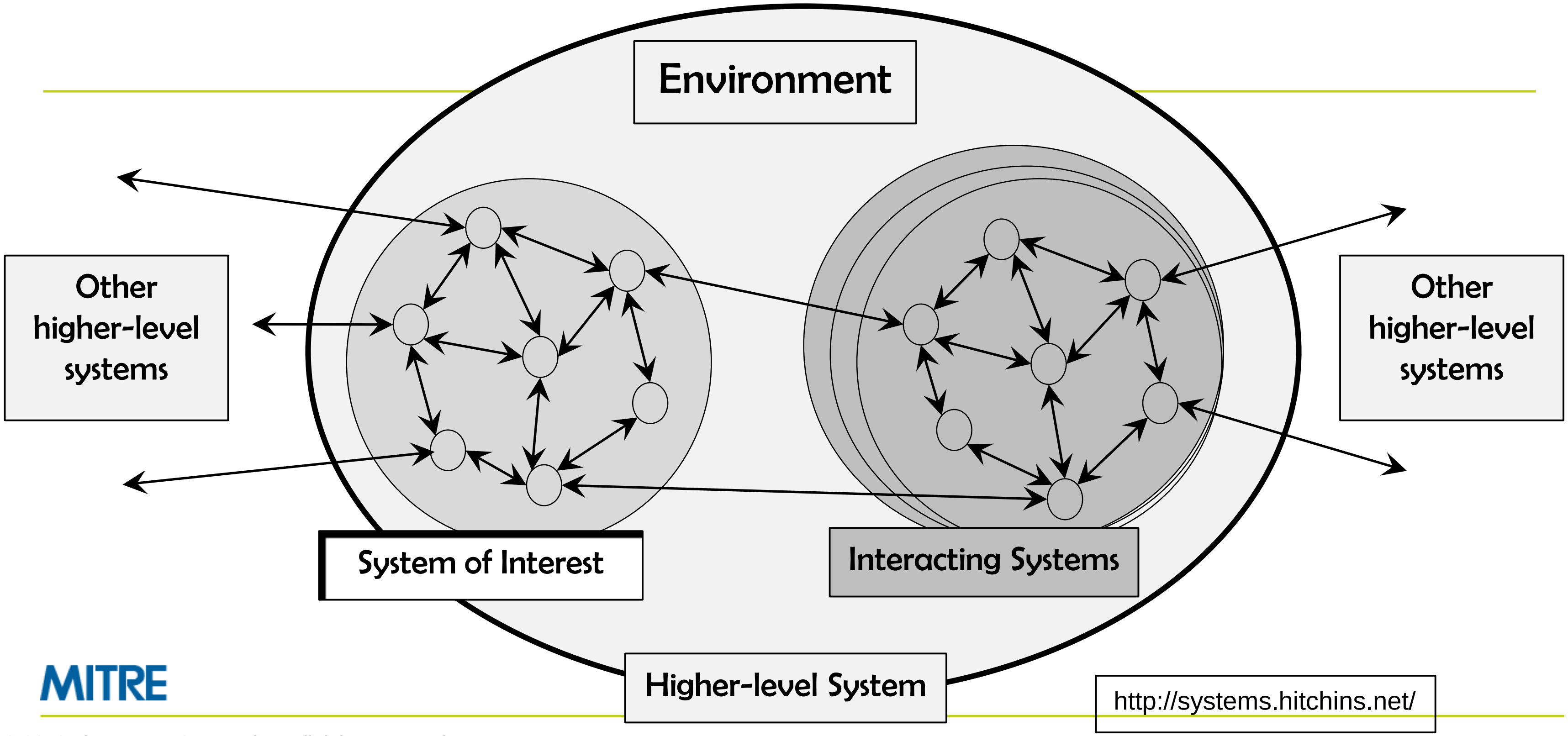
= **Adequate Security**

These essentials form the foundation of secure systems

MITRE

A Systems-Oriented Way Forward

Context-driven control over system behavior, interactions, and outcomes to limit the extent of loss and adverse consequences for stakeholder and system assets



MITRE

Security, Secure System, Adequately Secure System

Adapted from NASA System Safety Handbook

- **Security**
  - Freedom from those conditions that can cause loss of assets with unacceptable consequences
    - A stakeholder determination
- **Secure System**
  - A system that for all identified states, modes, and transitions is deemed secure
    - i.e., demonstrates "freedom from those conditions ..."
- **Adequately Secure System**
  - Adequately secure is an evidence-based determination that weighs system security performance against all other performance objectives and constraints

Safety
Safety is freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. In any given application, the specific scope of safety must be clearly defined by the stakeholders in terms of the entities to which it applies and the consequences against which it is assessed. For example, for non-reusable and/or non-recoverable systems, damage to or loss of equipment may be meaningful only insofar as it translates into degradation or loss of mission objectives.

MITRE

Relationships
Asset, Loss, Context, and Consequence

Types of Asset

- Humans
- Data and information
- Sensitive, proprietary, privacy data and information
- Components, elements
- Assemblies, subsystems
- Systems, system-of-systems
- Infrastructure
- Capability
- Processes, procedures
- Provision of service or function
- Intellectual property
- Technological, competitive, combatant advantage
- Image
- Reputation
- Trust

Form of Asset Loss

- Ability, capability
- Accessibility
- Accuracy, precision
- Advantage (combatant, competitive, technological)
- Assurance
- Control
- Correctness
- Existence
- Investment
- Ownership
- Performance
- Possession
- Quality
- Satisfaction
- Time

CONTEXT

CONSEQUENCE

Context is at the Core of Interpretation of Loss

Correlation between asset and form of loss is necessary to properly differentiate and to reason

MITRE

Predominate Views of System Security

- **Security Function of the System**
  - Security functions that provide system protection capability
    - Mechanisms, safeguards, countermeasures, features, controls, overrides, inhibits

- **Security of the Intended System Function**
  - Security-driven constraints for all system functions
    - Avoid, eliminate, tolerate defects, exposure, flaws, weaknesses

- **Security of Life Cycle Assets**
  - Security for data, information, technology, methods, and other assets associated with the system throughout its life cycle

MITRE

Differentiating
Security Protection and System Security

System Security

Emergent property of the system deemed to be trustworthy and adequate

Security Protection

Behavioral & Non-behavioral Aspects

Composition of Security Protections

Composition of Security Protections

What the system has or does not have

What the system does and does not do

Defined and assessed based on concerns of asset loss and the associated consequences

System Security and Failure

- **Security failure results in asset loss or adverse consequence**
  - Exhibiting unspecified behavior or interactions
  - Producing unspecified outcomes

- **Can be forced or unforced**
  - Forced security failure results from malicious activities with intent to cause harm
    - Human attacks and abuse
  - Unforced security failure results from non-malicious activities and events
    - Machine and technology errors and faults
    - Incidents and accidents
    - Human errors of omission and commission
    - Human misuse
    - Environmental and disaster events

Failure is related to system modes, states, and transitions

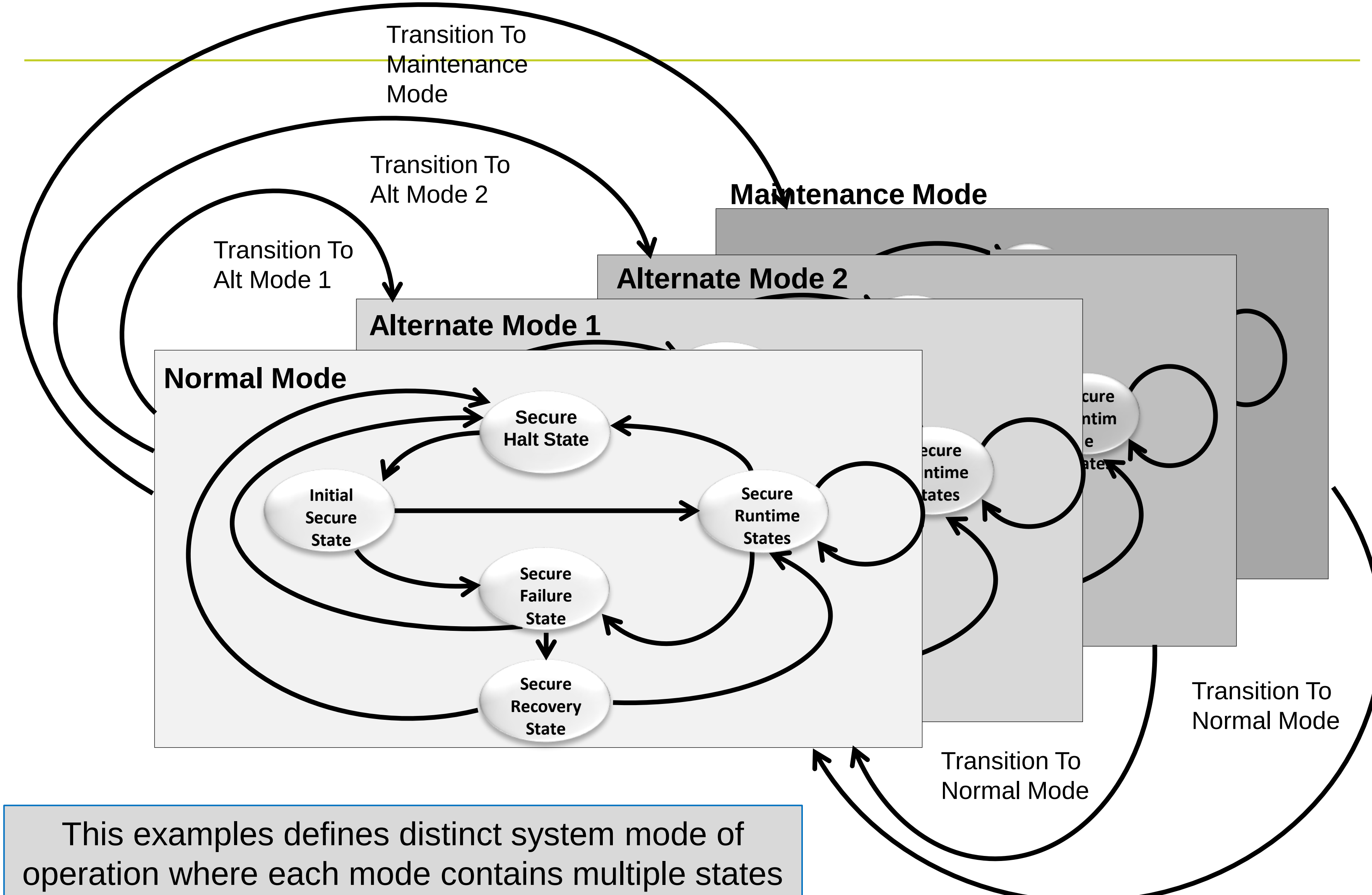
Secure Modes, States, Transitions

- **A secure system remains secure for all modes, states and transitions**
  – To include the halt state/mode
- **Additional states, modes, and transitions reflect concepts of:**
  – Failure with preservation of secure state/mode
    - The ability to detect that the system is in a non-secure state/mode or to detect a transition that will place the system in a non-secure state/mode
  – Trusted recovery
    - The ability to effect reactive, responsive, or corrective action to securely transition from a non-secure state/mode to a secure state/mode (or some less insecure state/mode)

MITRE

Secure Modes, States, and Transitions

Example: Idealized Secure System

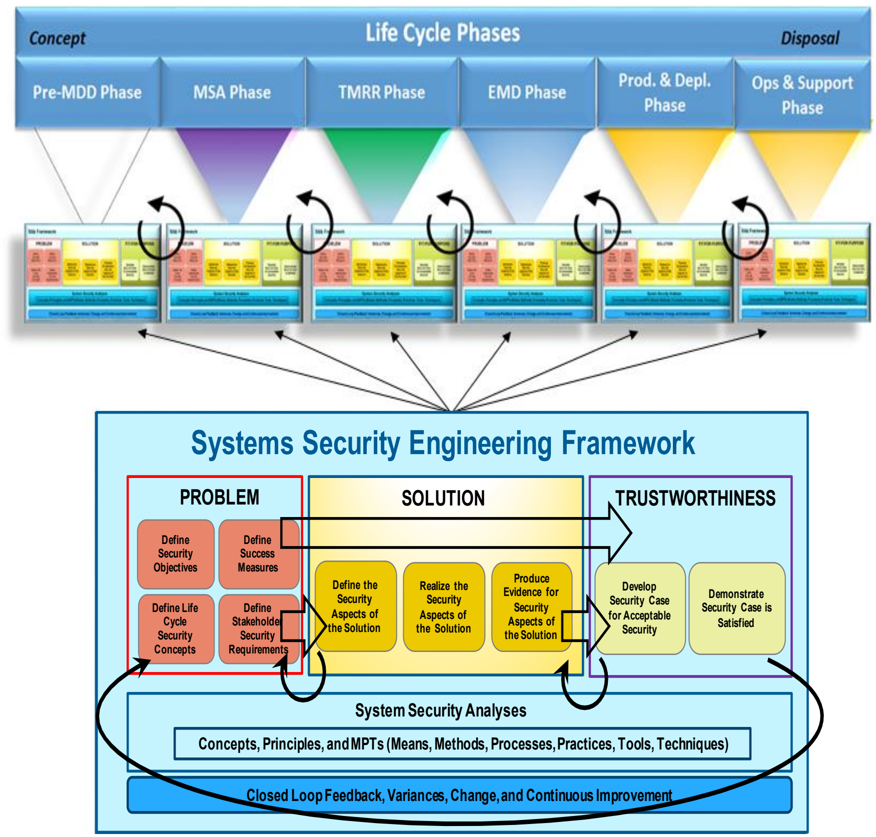


This examples defines distinct system mode of operation where each mode contains multiple states

MITRE

System Security Trustworthiness

- **Maintain a statement of trustworthiness across needs and variances**
  - All systems do not have the same fidelity and rigor trustworthiness needs
  - Adequate security expressed by security claims
  - Relevant and credible evidence
  - Appropriate fidelity and rigor
  - Valid arguments that relate all evidence to security claims
  - Analyses by subject matter experts



Enabled by System Analysis – Focused on Asset and Loss Consequences

Systems Security Engineering in a Nutshell

Controlling the loss and associated consequences of stakeholder and system assets while realizing stakeholder capability objectives throughout the life cycle

Security Functions	**Engineers the active and passive protection capability of the system**
System Functions	**Engineers the security-driven constraints for the entire system to limit security-relevant defects**
Life Cycle Assets	**Engineers the protection for stakeholder and system data, information, technology, and method assets**

Delivers trustworthy secure systems
Develops the design oriented to objectives and success measures
Decision-making informed by data and analyses with appropriate fidelity and rigor

Constrained by the laws of physics and the laws of computational logic

800-160 Way Forward

- **Special Publication 800-160 will become the flagship publication for the NIST Systems Security Engineering Initiative.**
  – Other NIST and Joint Task Force (JTF) publications will leverage 800-160 in future revisions
- **The following supporting NIST publications will be developed and published in 2017 and beyond:**
  – Special Publication 800-160A, Systems Security Engineering: Considerations for System Resilience in the Engineering of Trustworthy Secure Systems
  – Special Publication 800-160B, Systems Security Engineering: Considerations for Software Assurance in the Engineering of Trustworthy Secure Systems
  – Special Publication 800-160C, Systems Security Engineering: Considerations for Hardware Assurance in the Engineering of Trustworthy Secure Systems
- **Risk Management Framework interaction with the life cycle processes to be described in future updates to NIST Special Publication 800-37**

On-target for December 2016 Release 1 Publication

Acknowledgements

- **Motivation for talk**
  - "*Putting the 'Systems' in Security Engineering: An Examination of NIST Special Publication 800-160",* IEEE Security & Privacy, July/August 2016
    - Logan O. Mailloux, Stephen Khou, John Pecarina; Air Force Institute of Technology
    - Michael McEvilley; The MITRE Corporation

- **NIST SP800-160 authors appreciate the ongoing support, review, commentary, and wish to thank**
  - DASD/SE: Ms. Kristen Baldwin, Ms. Melinda Reed
  - INCOSE, NDIA: SSE WG Chairs and Team Members

MITRE