CYBERSECURITY: VERIFICATION AND VALIDATION, AND DEVELOPMENTAL AND OPERATIONAL TEST & EVALUATION

20181001 (BREFLET 013)

David Olmstead, PE, ESEP, CISSP-ISSEP, CPP, C|EH
Systems Engineer, Senior Staff

LOCKHEED MARTIN

SYSTEM SECURITY SYSTEMS ENGINEERING

MFC CYBER SECURITY

SYSTEMS ENGINEERING

PERMIT ME TO INTRODUCE MYSELF,

David Olmstead
Systems Engineer, Senior Staff
Systems Security Specialty Engineering

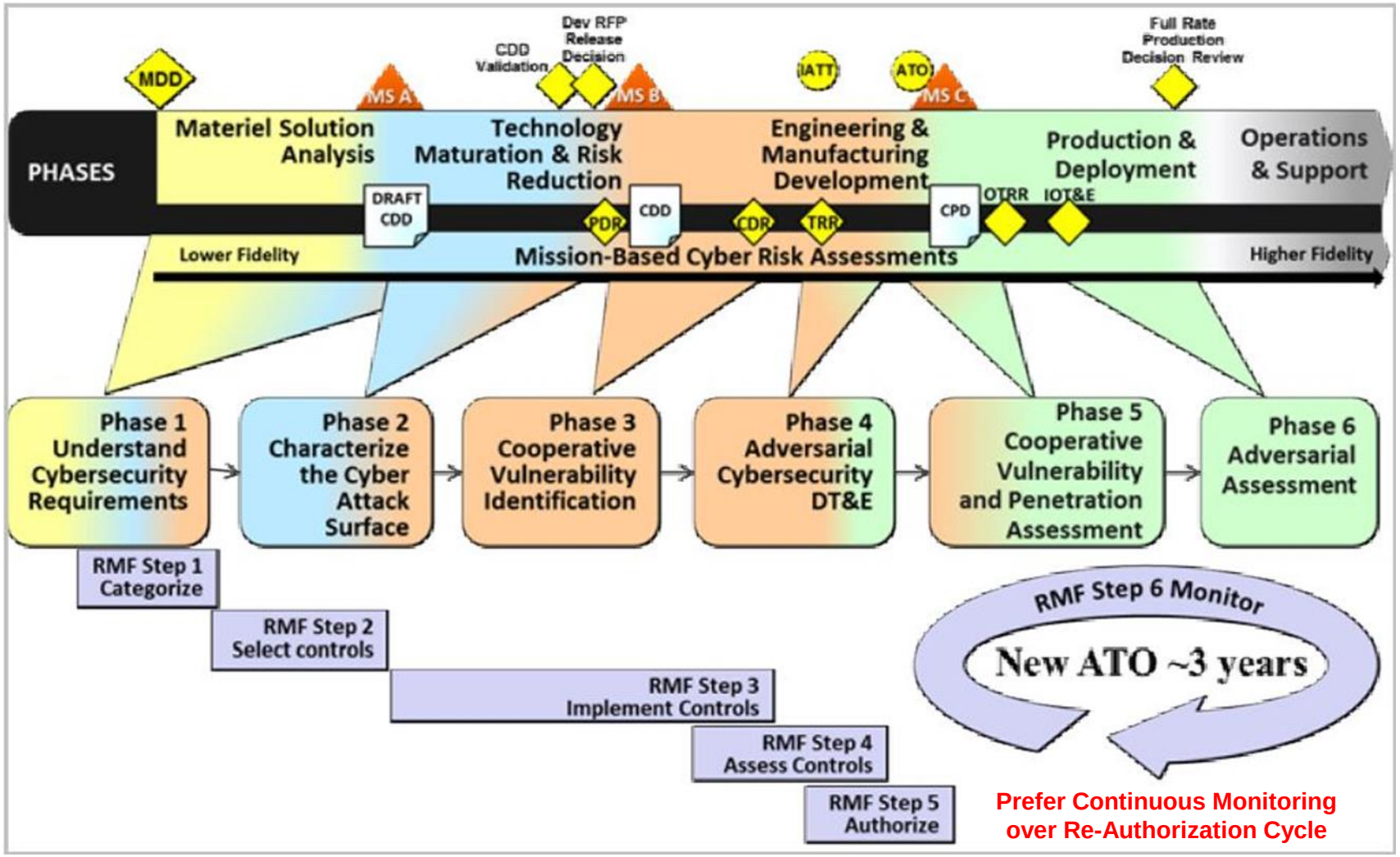
Lockheed Martin Missiles and Fire Control
5600 Sand Lake Road, MP-914, Orlando, FL 32819-1380

Email: david.olmstead@lmco.com
Phone: 407-356-4526

BOTTOM LINE UP FRONT (BLUF)

FIGURE 3-4. INTERACTION OF T&E AND RMF CYBERSECURITY ACTIVITIES

- T&E activities are Blue Book-Team / Red Team-Book
  - Integrate Cyber Adversarial Context into the DOT&E TEMP
- RMF activities are Specification TADIC-P driven
  - Always Achieve Specification Compliance or Obtain Deviation / Waver for Non-Compliance

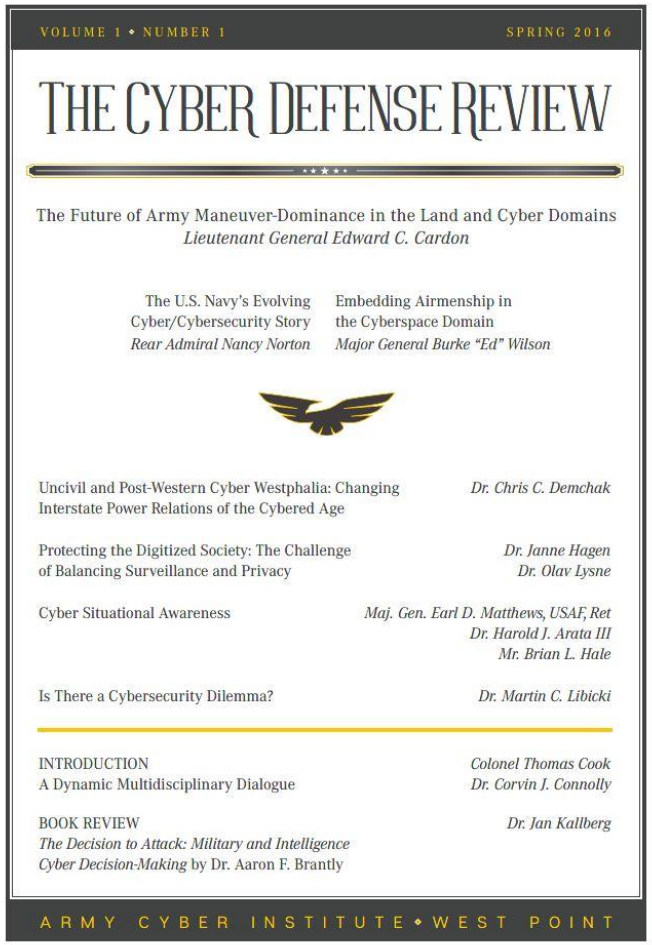


PARALLEL CYBERSECURITY V&V AND T&E

- System Survivability KPP (w/Cyber Survivability – Resiliency)
- Director Operational Test and Evaluation (DOT&E) Test and Evaluation Master Plan (TEMP) “testing” (& Cyber T&E Guidebook v2.0)
  - **Developmental T&E; evidence (Blue Book/Team) you are making progress**
  - **Operational T&E; evidence (Red Team/Book) you have Resiliency**

- Cybersecurity System, Sub-System, and Product Specification §4
- IEEE Std 1012™-2016, IEEE Standard for System And Software Verification and Validation “testing”
  - **Verification; evidence you built the thing right**
  - **Validation; evidence you built the right thing**
  - **Continuous Monitoring for Cyber in Operations and Support (O&S) Phase(?)**

THE BLUE BOOK/TEAM AND RED TEAM/BOOK



VOLUME 1 • NUMBER 1 SPRING 2016

THE CYBER DEFENSE REVIEW

The Future of Army Maneuver-Dominance in the Land and Cyber Domains
Lieutenant General Edward C. Cardon

The U.S. Navy's Evolving Cyber/Cybersecurity Story
Rear Admiral Nancy Norton

Embedding Airmenship in the Cyberspace Domain
Major General Burke "Ed" Wilson

Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age — *Dr. Chris C. Demchak*

Protecting the Digitized Society: The Challenge of Balancing Surveillance and Privacy — *Dr. Janne Hagen, Dr. Olav Lysne*

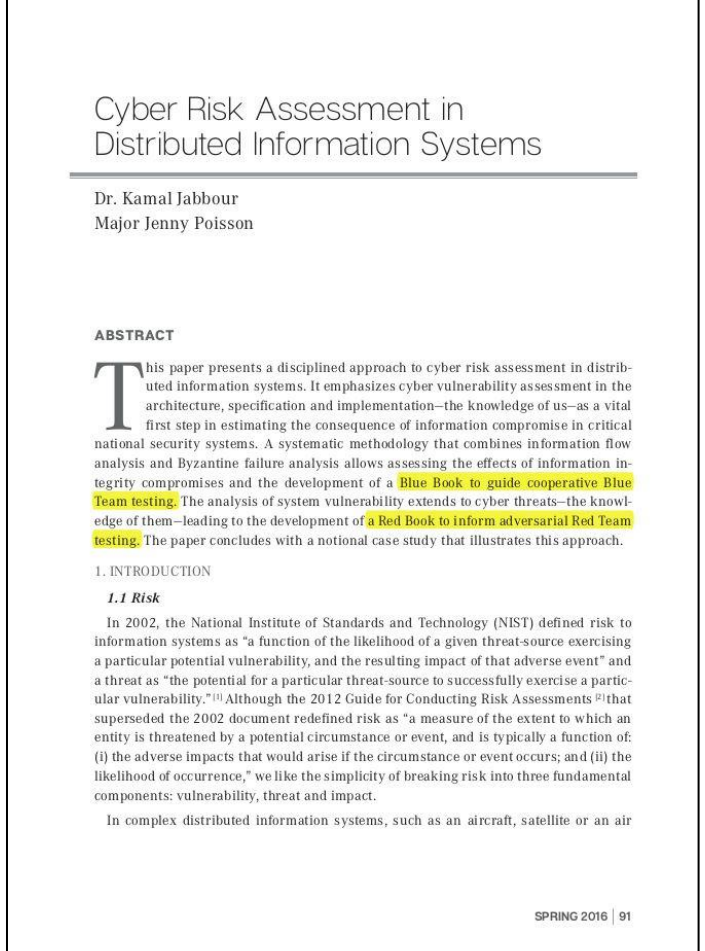
Cyber Situational Awareness — *Maj. Gen. Earl D. Matthews, USAF, Ret, Dr. Harold J. Arata III, Mr. Brian L. Hale*

Is There a Cybersecurity Dilemma? — *Dr. Martin C. Libicki*

INTRODUCTION
A Dynamic Multidisciplinary Dialogue — *Colonel Thomas Cook, Dr. Corvin J. Connolly*

BOOK REVIEW
The Decision to Attack: Military and Intelligence Cyber Decision-Making by Dr. Aaron F. Brantly — *Dr. Jan Kallberg*

ARMY CYBER INSTITUTE • WEST POINT



Cyber Risk Assessment in Distributed Information Systems

Dr. Kamal Jabbour
Major Jenny Poisson

ABSTRACT

This paper presents a disciplined approach to cyber risk assessment in distributed information systems. It emphasizes cyber vulnerability assessment in the architecture, specification and implementation—the knowledge of us—as a vital first step in estimating the consequence of information compromise in critical national security systems. A systematic methodology that combines information flow analysis and Byzantine failure analysis allows assessing the effects of information integrity compromises and the development of a Blue Book to guide cooperative Blue Team testing. The analysis of system vulnerability extends to cyber threats—the knowledge of them—leading to the development of a Red Book to inform adversarial Red Team testing. The paper concludes with a notional case study that illustrates this approach.

1. INTRODUCTION

1.1 Risk

In 2002, the National Institute of Standards and Technology (NIST) defined risk to information systems as "a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event" and a threat as "the potential for a particular threat-source to successfully exercise a particular vulnerability."[1] Although the 2012 Guide for Conducting Risk Assessments [2] that superseded the 2002 document redefined risk as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence," we like the simplicity of breaking risk into three fundamental components: vulnerability, threat and impact.

In complex distributed information systems, such as an aircraft, satellite or an air

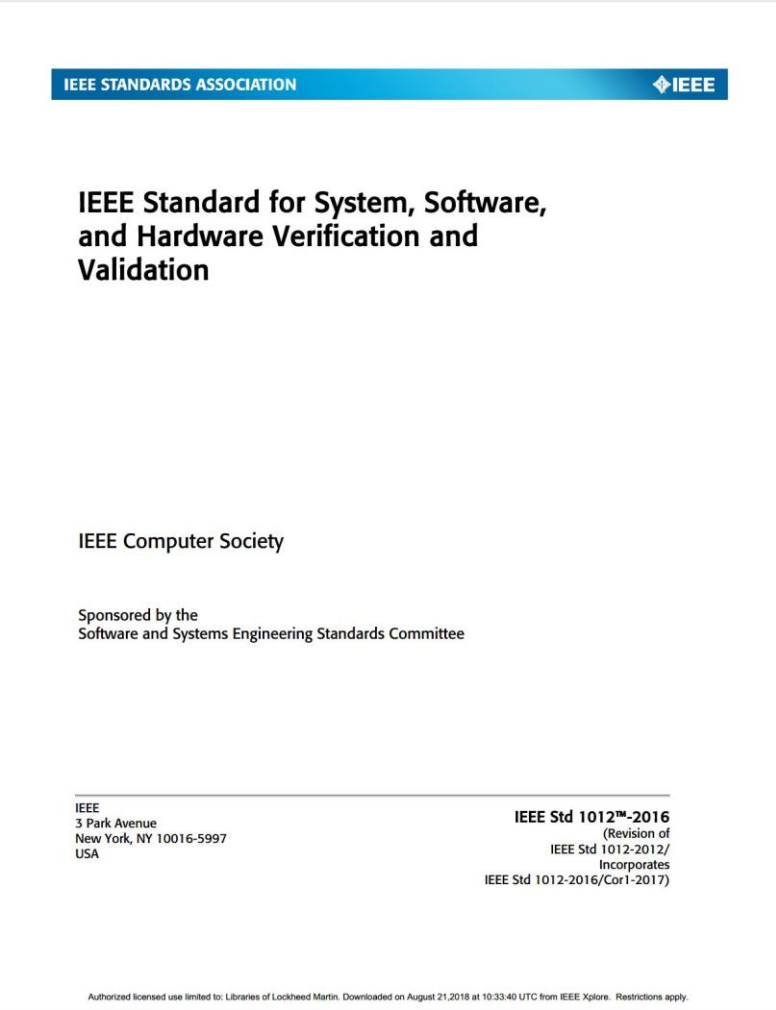
SPRING 2016 | 91

- The Cyber Risk Assessment (a roadmap)
- Byzantine exploitation
- Separate Vulnerability
  - **Impact or the What**
  - **From Threat or the How**

- http://www.dtic.mil/docs/citations/ADA635475
- http://www.dtic.mil/dtic/tr/fulltext/u2/a635475.pdf

Product Life Cycle Centered Mission Based Cyber Risk Assessment (MBCRA)

IEEE STD 1012™-2016



IEEE STANDARDS ASSOCIATION ◆IEEE

IEEE Standard for System, Software, and Hardware Verification and Validation

IEEE Computer Society

Sponsored by the
Software and Systems Engineering Standards Committee

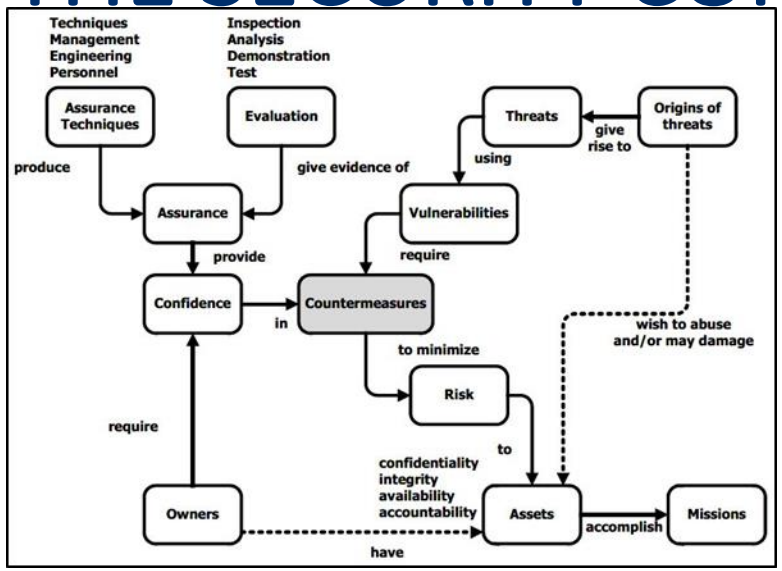
IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 1012™-2016
(Revision of
IEEE Std 1012-2012/
Incorporates
IEEE Std 1012-2016/Cor1-2017)

- Verification and validation (V&V) processes are used to determine whether the development products of a given activity conform to the requirements of that activity and whether the product satisfies its intended use and user needs.
- V&V life cycle process requirements are specified for different integrity levels.
- The scope of V&V processes encompasses systems, software, and hardware, and it includes their interfaces.
- This standard applies to systems, software, and hardware being developed, maintained, or reused (legacy, commercial off-the-shelf [COTS], non-developmental items).
- The term software also includes firmware and microcode, and each of the terms system, software, and hardware includes documentation.
- V&V processes include the analysis, evaluation, review, inspection, assessment, and testing of products.

Cybersecurity is "Built Into" Verification and Validation

IEEE STD 1012™-2016, FIGURE J.1
THE SECURITY CONTEXT OF THE SYSTEM



There are two (2) entrances to "Countermeasures"

- **"Baseline" Assurance to give Owners Confidence in the System-of-Interest**
- **Threats that use Vulnerabilities and Require Countermeasures**

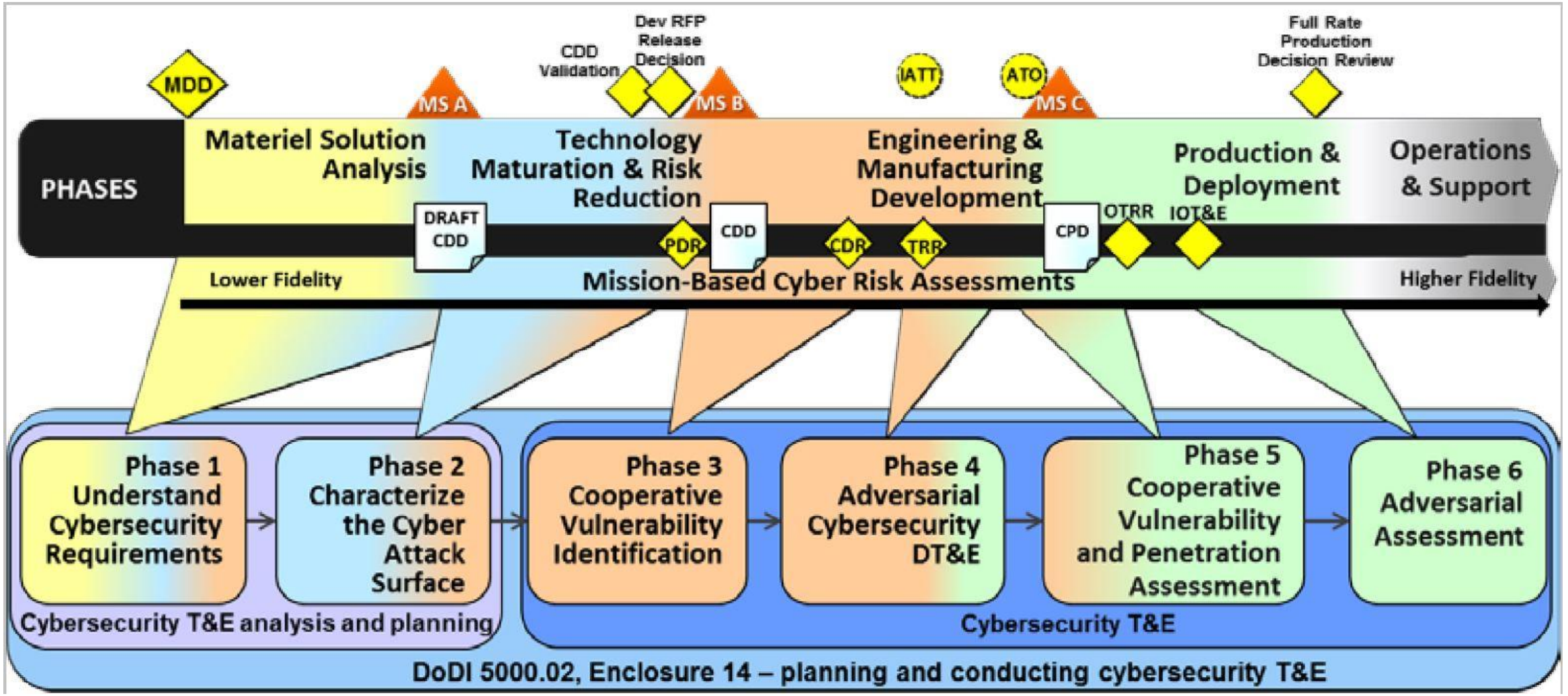
Both are "Mission Driven"

- One of the objectives of security analysis performed by the V&V effort is to verify that the system-required threat controls and safeguards are correctly implemented and to validate that they provide the desired levels of protection of system vulnerabilities. The other objective is to verify that there is a process for describing the system, software, and hardware process security.
- A system should consider different security issues in each phase of the life cycle because the system owner may change as the product evolves. The V&V security analysis should consider:
  - **The context of the system (e.g., the development process and environment, the final operational environment, organization structures and management policy, operational and maintenance personnel roles, interfaces with other external systems or support systems);**
  - **The system of interest and its elements, threats, vulnerabilities, and countermeasures;**
  - **Tradeoffs between techniques, operations, and management to address security requirements.**
  - **Identification of threats. These threats may be natural (e.g., inclement weather, earthquakes), human (e.g., unintended or malicious), or environmental (e.g., chemical leak, power loss).**

Cybersecurity (i.e., Security Context) is "Built Into" Verification and Validation

TEST AND EVALUATION (T&E)
BLUE BOOK-TEAM / RED TEAM-BOOK

T&E GUIDEBOOK FIGURE 3-1. CYBERSECURITY T&E PHASES MAPPED TO THE ACQUISITION LIFE CYCLE



CYBERSECURITY T&E PHASE DESCRIPTION (1 AND 2)

- **Phase 1—Understand the Cybersecurity Requirements. The purpose of the first phase is to examine the system's cybersecurity and resilience requirements for developing an initial approach and plan for conducting cybersecurity T&E.**
- **Phase 2—Characterize the Attack Surface. The purpose of the second phase is to identify vulnerabilities and avenues of attack an adversary may use to exploit the system and to develop plans to evaluate the impact to the mission.**
- **These two phases define the "who, what, where, when, why, and how" for testing, including the scope of the test, required test tools and infrastructure, and requisite skills of the representative opposing force (OPFOR).**

Technology Maturation & Risk Reduction (TMRR) Early Operational Assessment (EOA)

CYBERSECURITY T&E PHASE DESCRIPTION (3 AND 4)

- Phase 3—Cooperative Vulnerability Identification. The purpose of the third phase is to verify cybersecurity and resilience and identify vulnerabilities and needed mitigations, which will inform system designers, developers, and engineers of needed cyber survivability and resilience improvements to reduce risk.
- Phase 4—Adversarial Cybersecurity DT& E. During this phase, an adversarial team tests the system's cybersecurity and resilience using a mission context and in a cyber-contested operating environment using realistic threat exploitation techniques to identify residual risk.
- Phases 3 and 4 comprise cybersecurity DT&E execution activities for the system. Cybersecurity testers develop test objectives, plan test activities and events, and plan the cybersecurity test infrastructure for Phases 3 and 4 based on the outcomes from the Phases 1 and 2 analyses.

Engineering and Manufacturing Development (EMD) Operational Assessment (OA)

CYBERSECURITY T&E PHASE DESCRIPTION (5 AND 6)

- Phase 5—Cooperative Vulnerability and Penetration Assessment. The purpose of this phase is to fully characterize the cybersecurity and resilience status of a system in a fully operational context and provide reconnaissance of the system in support of AA.
- Phase 6—Adversarial Assessment. Phase 6 characterizes the operational mission effects to critical missions caused by threat-representative cyber activity against a unit trained and equipped with a system, as well as the effectiveness of defensive capabilities.
- Phases 5 and 6 comprise cybersecurity OT&E activities for the system. Cybersecurity operational testers provide the information needed to resolve operational cybersecurity issues, identify vulnerabilities in a mission context, and describe operational effects of discovered vulnerabilities.

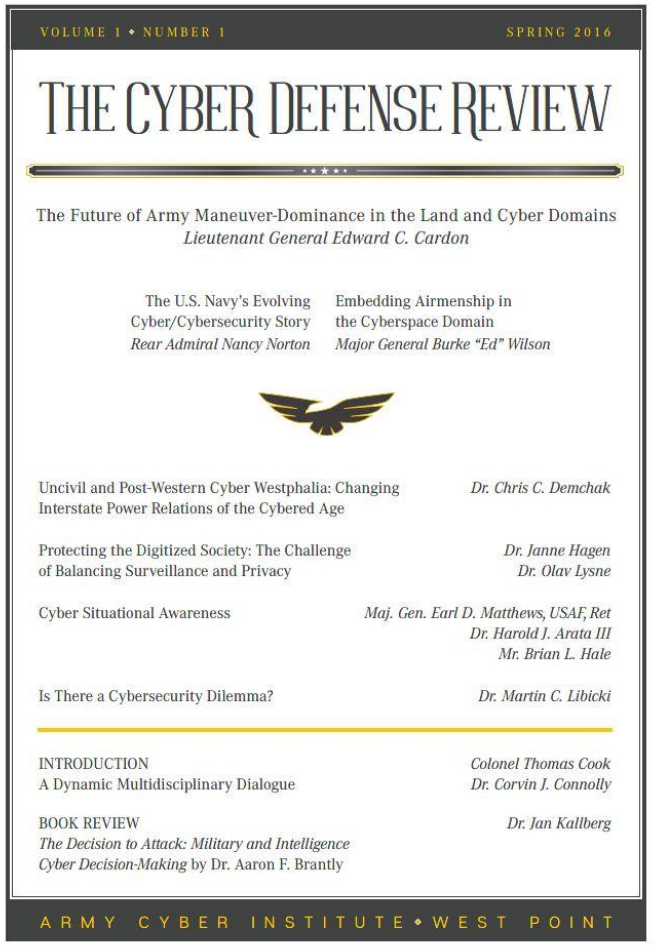
Production & Deployment (P&D) Initial/Follow-on Operational Test & Evaluation (I/FOT&E)

MISSION-BASED CYBER RISK ASSESSMENTS (MBCRA)

- Often is not possible to address all vulnerabilities, susceptibilities, and exploitable attack paths before a system is fielded, the Cybersecurity Working Group plans and conducts an MBCRA beginning in Phase 1 to focus and prioritize the Cybersecurity T&E effort.
- MBCRA is a process for identifying, estimating, assessing, and prioritizing risks based on impacts to DoD operational missions resulting from cyber effects on the system(s) employed.
- Recognizing MBCRAs as a best practice and a recommended tool, Section 3.1, Figure 3-1 (above) depicts MBCRAs across the acquisition life cycle with increasing fidelity as the system design matures.
- The employment of “Blue Teams” for Cooperative Vulnerability identification and verification followed by “Red Team” independent Adversarial Assessments

MBCRA is Applied against the Cybersecurity BASELINE (Doesn't Replace Baseline)

THE BLUE BOOK/TEAM AND RED TEAM/BOOK



VOLUME 1 • NUMBER 1 SPRING 2016

THE CYBER DEFENSE REVIEW

The Future of Army Maneuver-Dominance in the Land and Cyber Domains
Lieutenant General Edward C. Cardon

The U.S. Navy's Evolving Cyber/Cybersecurity Story
Rear Admiral Nancy Norton

Embedding Airmenship in the Cyberspace Domain
Major General Burke "Ed" Wilson

Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age — *Dr. Chris C. Demchak*

Protecting the Digitized Society: The Challenge of Balancing Surveillance and Privacy — *Dr. Janne Hagen, Dr. Olav Lysne*

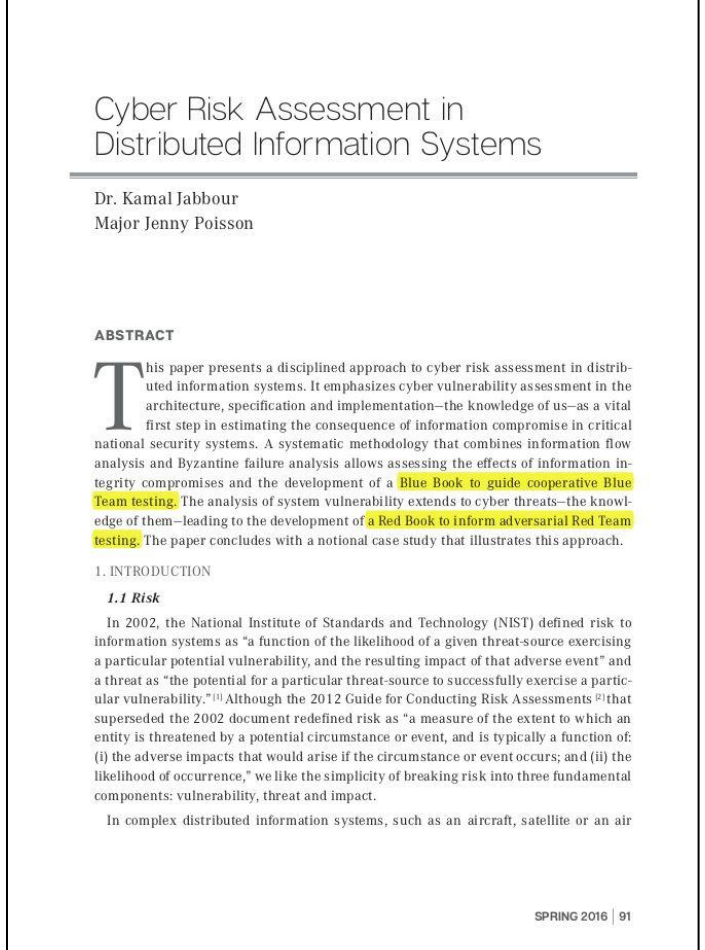
Cyber Situational Awareness — *Maj. Gen. Earl D. Matthews, USAF, Ret, Dr. Harold J. Arata III, Mr. Brian L. Hale*

Is There a Cybersecurity Dilemma? — *Dr. Martin C. Libicki*

INTRODUCTION
A Dynamic Multidisciplinary Dialogue — *Colonel Thomas Cook, Dr. Corvin J. Connolly*

BOOK REVIEW
The Decision to Attack: Military and Intelligence Cyber Decision-Making by Dr. Aaron F. Brantly — *Dr. Jan Kallberg*

ARMY CYBER INSTITUTE • WEST POINT



Cyber Risk Assessment in Distributed Information Systems

Dr. Kamal Jabbour
Major Jenny Poisson

ABSTRACT

This paper presents a disciplined approach to cyber risk assessment in distributed information systems. It emphasizes cyber vulnerability assessment in the architecture, specification and implementation—the knowledge of us—as a vital first step in estimating the consequence of information compromise in critical national security systems. A systematic methodology that combines information flow analysis and Byzantine failure analysis allows assessing the effects of information integrity compromises and the development of a Blue Book to guide cooperative Blue Team testing. The analysis of system vulnerability extends to cyber threats—the knowledge of them—leading to the development of a Red Book to inform adversarial Red Team testing. The paper concludes with a notional case study that illustrates this approach.

1. INTRODUCTION

1.1 Risk

In 2002, the National Institute of Standards and Technology (NIST) defined risk to information systems as "a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event" and a threat as "the potential for a particular threat-source to successfully exercise a particular vulnerability."[1] Although the 2012 Guide for Conducting Risk Assessments [2] that superseded the 2002 document redefined risk as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence," we like the simplicity of breaking risk into three fundamental components: vulnerability, threat and impact.

In complex distributed information systems, such as an aircraft, satellite or an air

SPRING 2016 | 91

- The Cyber Risk Assessment (a roadmap)
- Byzantine exploitation
- Separate Vulnerability
  - **Impact or the What**
  - **From Threat or the How**
  - http://www.dtic.mil/docs/citations/ADA635475
  - http://www.dtic.mil/dtic/tr/fulltext/u2/a635475.pdf

Product Life Cycle Centered Mission Based Cyber Risk Assessment (MBCRA)

BLUE BOOK, BLUE TEAM TESTING AGAINST CYBER BASELINE (CONNECT THE SUSCEPTIBILITY TO THE MISSION IMPACT)

- Apply Byzantine White Box failure analysis to separate the impact of a failure from its root-cause threat
- The Systems Engineering design team products an introspective “Blue Book” of potential Cybersecurity design “Operational Susceptibilities”
- The Corporative “Blue Team”, guided by the Blue Book, validate or repudiate the hypotheses relating to the postulated operational susceptibilities based on Byzantine exploitation
- Blue Team Testing Purpose:
  - **First, they inform the adversarial Red Team on which information compromises to pursue maliciously**
  - **Second, they advise the mission owner on cyber risk to the mission**
  - **Third, they establish a roadmap for mitigation efforts based one the intent of the mission owner**

Blue Book Assumption: the System Developer Knows They Self Best

RED TEAM TESTING, RED BOOK (THREAT CHARACTERIZATION – CAPABILITIES AND MEANS)

- The Threat, represents
  - **The capability (time, talent and treasure) necessary to replicate the Blue Book impact in an adversarial manner**
  - **The adversarial access means (remote, physical, supply chain)**
  - **The intent which is assumed to exist in the Advanced Persistent Threat (APT)**
- The Initial Red Book defines the adversary capabilities necessary to exploit the Blue Book vulnerabilities
  - **See Cybersecurity Security Classification / Declassification Guide for Air Force Weapon Systems 20170417**
- The end product of Red Team testing is a "Red Book" of validated threat replication to exploit Blue Book vulnerabilities
  - **See Cybersecurity Security Classification / Declassification Guide for Air Force Weapon Systems 20170417**

Adversarial (White Hat) Test Community is High Demand Low Density (HDLD)

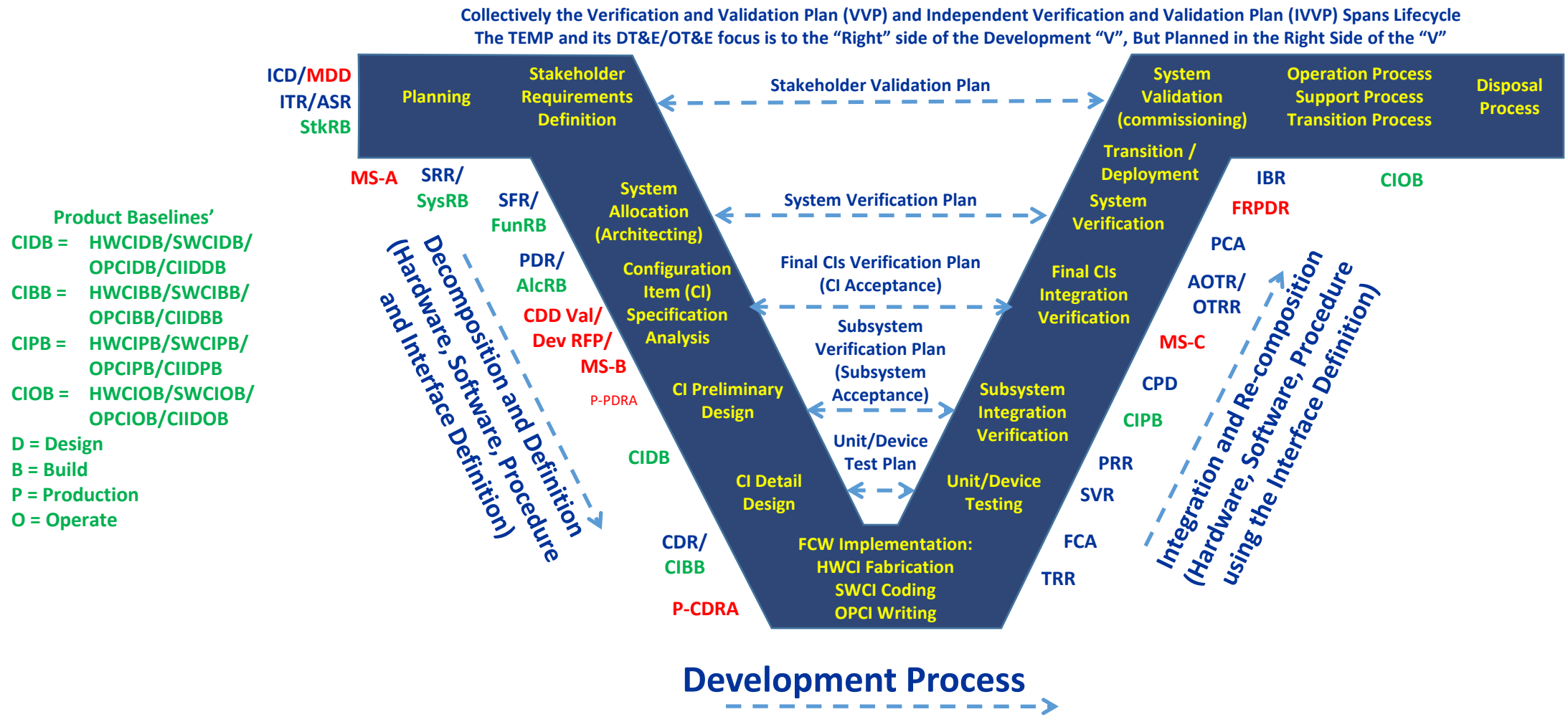
BLUE BOOK – RED BOOK

- **The goal of the Blue Team is to estimate the consequence of vulnerabilities independent of the cause**
  - The Blue Team performs corporative vulnerability testing (fuzz testing, penetration testing, etc.) to define consequences
- **The goal of the Red Team is to effect exploitation of Blue Book vulnerabilities through adversarial means**
  - The Red Team develops an Initial Red Book of adversary capabilities necessary to exploit the Blue Book vulnerabilities
  - The Initial Red Book provides the Red Team with a roadmap to conduct adversarial testing by a Red Team and define the threat capabilities that an aggressor team sought to understand, replicate and exercise.
  - The Final Red Book details the results of Red Team testing as guided by the Initial Red Book

Classification Level and Need-To-Know Restrictions Quickly Escalates During Testing

SPECIFICATION §4 VERIFICATION/VALIDATION

DoD AT&L PRODUCT LIFE CYCLE PROCESS



Nothing New; The original "V-Chart" was first presented at NCOSE (now INCOSE) in 1991

BASELINE LANGUAGE PROGRESSION CYBERSECURITY'S REQUIREMENT PROGRESS

Your Starting Point in the Process i.e., You Are Here

You get your Stakeholder Requirements from NIST SP 800-53r4 and their Verification from NIST SP 800-53Ar4 via CNSSI 1253

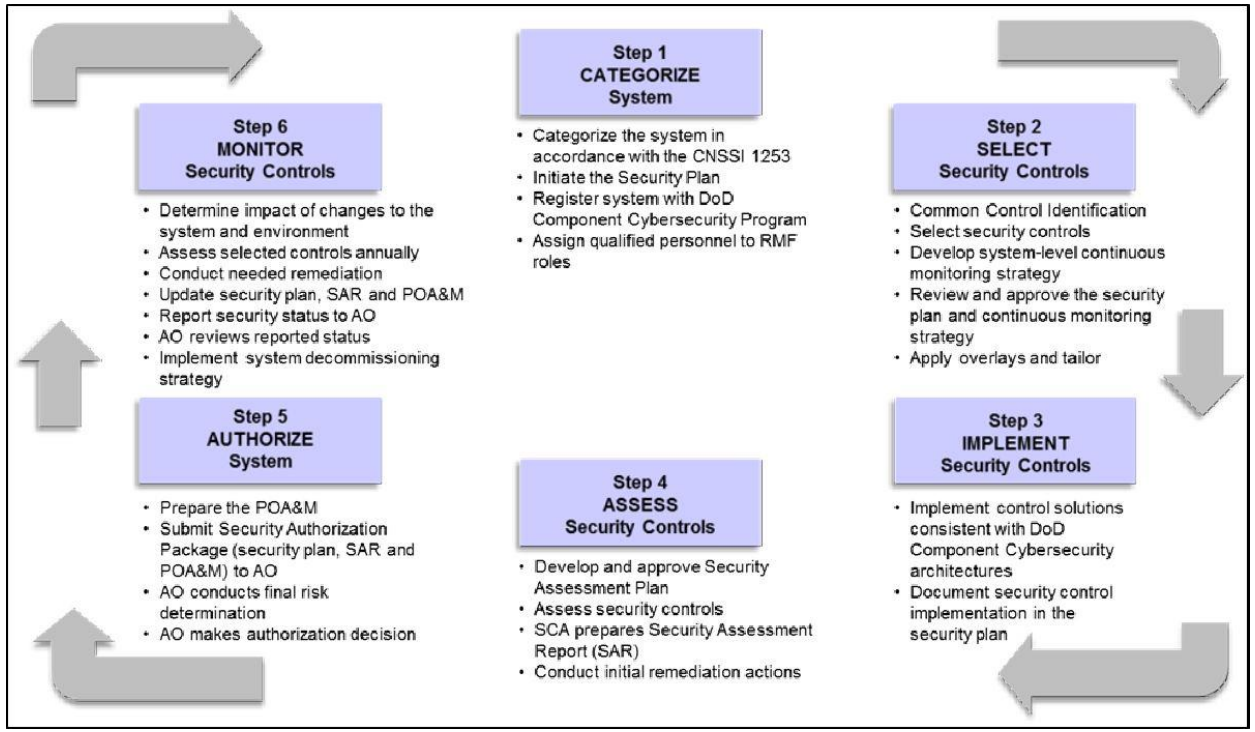
Stakeholder Requirements Baseline	Customer Speak	System Documents (Requirements Configuration)	Stakeholder Competing and Conflicting Requirements
System Requirements Specification	Agnostic System Speak	System Documents (Requirements Configuration)	Stakeholder Competing and Conflicting Requirements
Functional Requirements Baseline	Agnostic System Speak	System Documents (Requirements Configuration)	De-conflicted Inter- Intra-Stakeholder Requirements
Allocated Requirements Baseline	Domain System Speak	System Documents (Requirements Configuration)	HWCIs, SWCIs, OPCIs, CIIDs Requirement Specifications
F/C/W Design Baseline	Domain Design Speak	Domain Documents (Domain Configuration)	HWF Design, SWC Design OPW Design, IDF/C/W Design
Product Baseline	Domain Product Speak	Domain Documents (Product Configuration)	Fabricated, Coded and Written Configuration Items

If you don't include security from the beginning, you have "Sub-optimized" the system and created an "Un-Affordable" solution

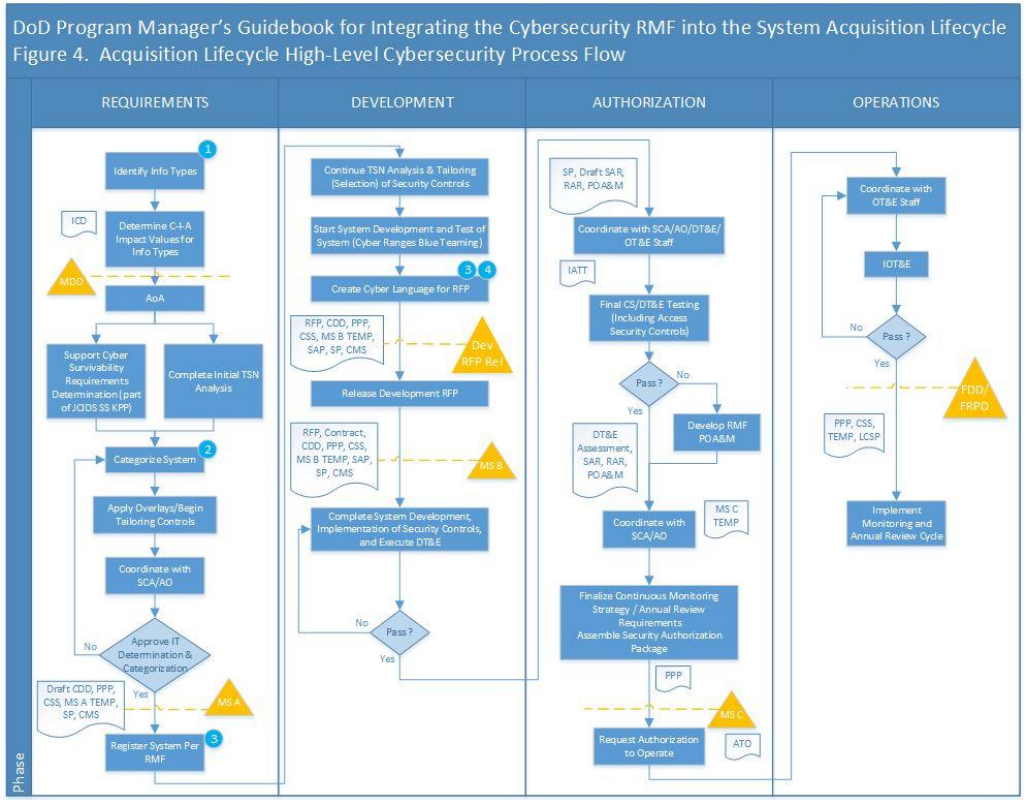
Cybersecurity's Position Along the Life Cycle Progression

DoD PM'S GUIDEBOOK FOR INTEGRATING THE CYBERSECURITY RMF INTO THE SYSTEM ACQUISITION LIFECYCLE

DoDI 8510.01 Enclosure 6, Figure 3, RMF for IS and PIT Systems

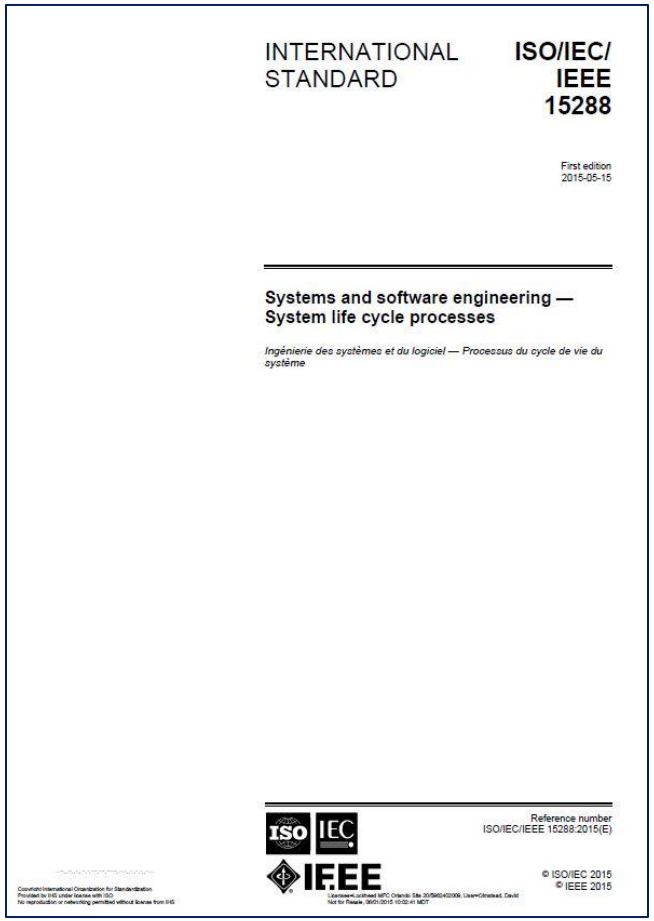


DoD PM's Guidebook Figure 4



Start With Good Requirements Engineering to Achieve Optimal Total System Solution

ISO/IEC/IEEE 15288-2015(E)



INTERNATIONAL STANDARD

ISO/IEC/ IEEE 15288

First edition
2015-05-15

Systems and software engineering — System life cycle processes

Ingénierie des systèmes et du logiciel — Processus du cycle de vie du système

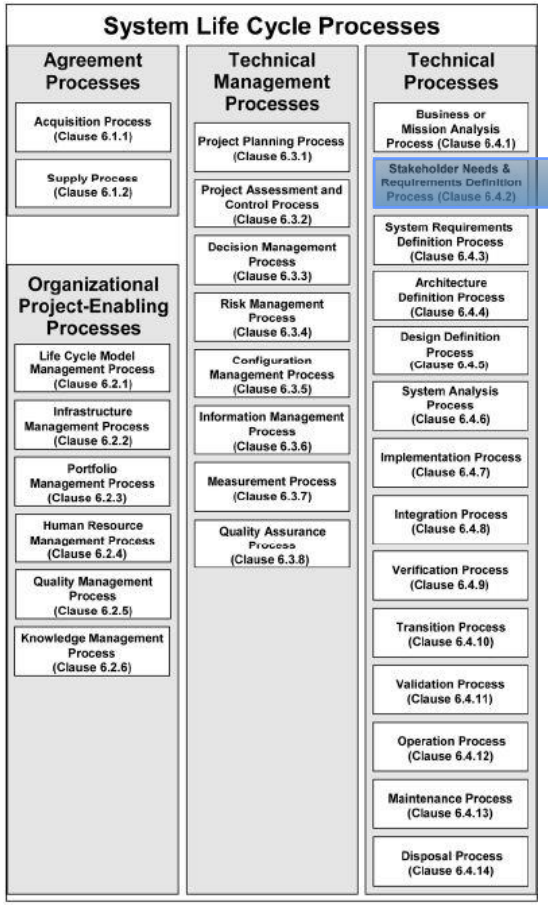
Reference number
ISO/IEC/IEEE 15288:2015(E)

© ISO/IEC 2015
© IEEE 2015

- **§6.4.2 Stakeholder Needs and Requirements Definition Process**
  - **The purpose of the Stakeholder Needs and Requirements Definition process is to define the stakeholder requirements for a system that can provide the capabilities needed by users and other stakeholders in a defined environment.**
    - Define Stakeholder Need includes: “Understanding stakeholder needs for the minimum security and privacy requirements necessary for the operational environment minimizes the potential for disruption in plans, schedules, and performance.”

The DoD Defined System Life Cycle Process Requirement

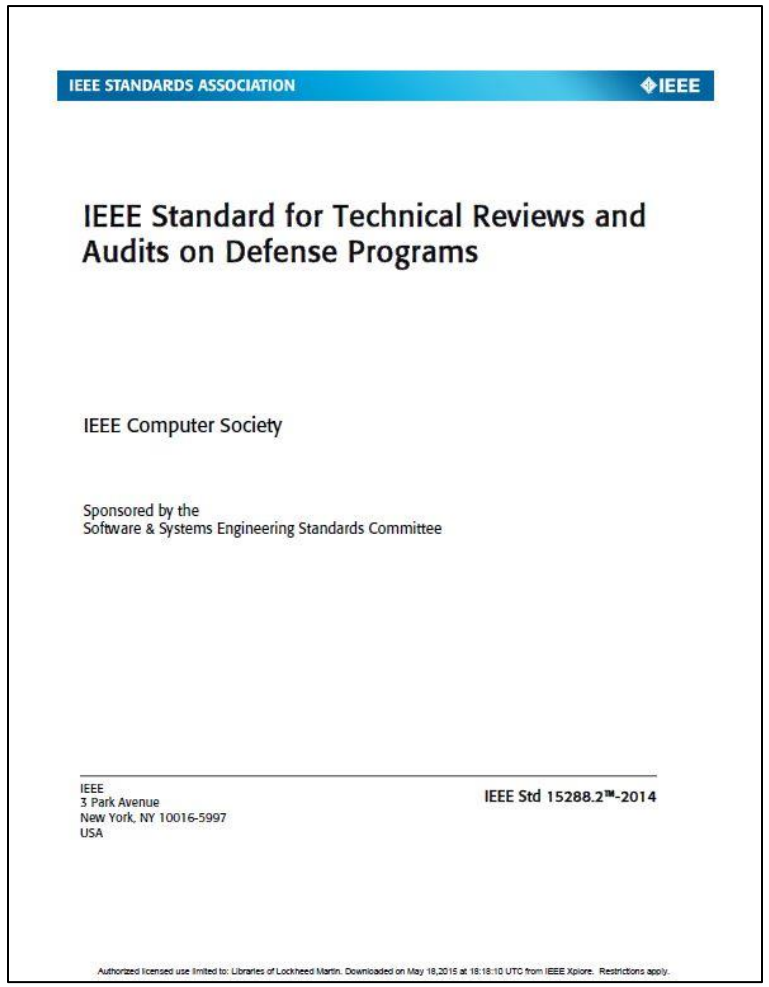
ISO/IEC/IEEE 15288-2015
THE REQUIREMENTS ENGINEER EARLY IN THE DEVELOPMENT



- **§6.4.2 Stakeholder Needs and Requirements Definition Process**
  - **6.4.2.3 Activities and tasks**
    - Note Some stakeholders have interests that oppose the system or oppose each other. When the stakeholder interests oppose each other, but do not oppose the system, this process is intended to gain consensus among the stakeholder classes to establish a common set of acceptable requirements
    - b) Define Stakeholder Needs.
      - 1) Define context of use within the concept of operations and the preliminary life cycle concepts
      - 2) Identify stakeholder needs
      - 3) Prioritize and down-select needs
      - 4) Define the stakeholder needs and rationale

Position within the Technical Processes

IEEE STD 15288.2™-2014


IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for Technical Reviews and Audits on Defense Programs

IEEE Computer Society

Sponsored by the
Software & Systems Engineering Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 15288.2™-2014

- This standard addresses the needs of the defense community with respect to the incorporation, implementation, and execution of technical reviews and audits. IEEE Std 15288.1-2014, the standard that implements ISO/IEC/IEEE 15288 for application on defense programs, provides the defense-specific language and terminology to ensure the correct application of acquirer-supplier requirements for technical reviews and audits on a defense program, while this standard provides the implementation details to fulfill those requirements.

Defense Program Technical Reviews and Audits

IEEE STD 15288.2™-2014 TECHNICAL REVIEW TO BASELINES

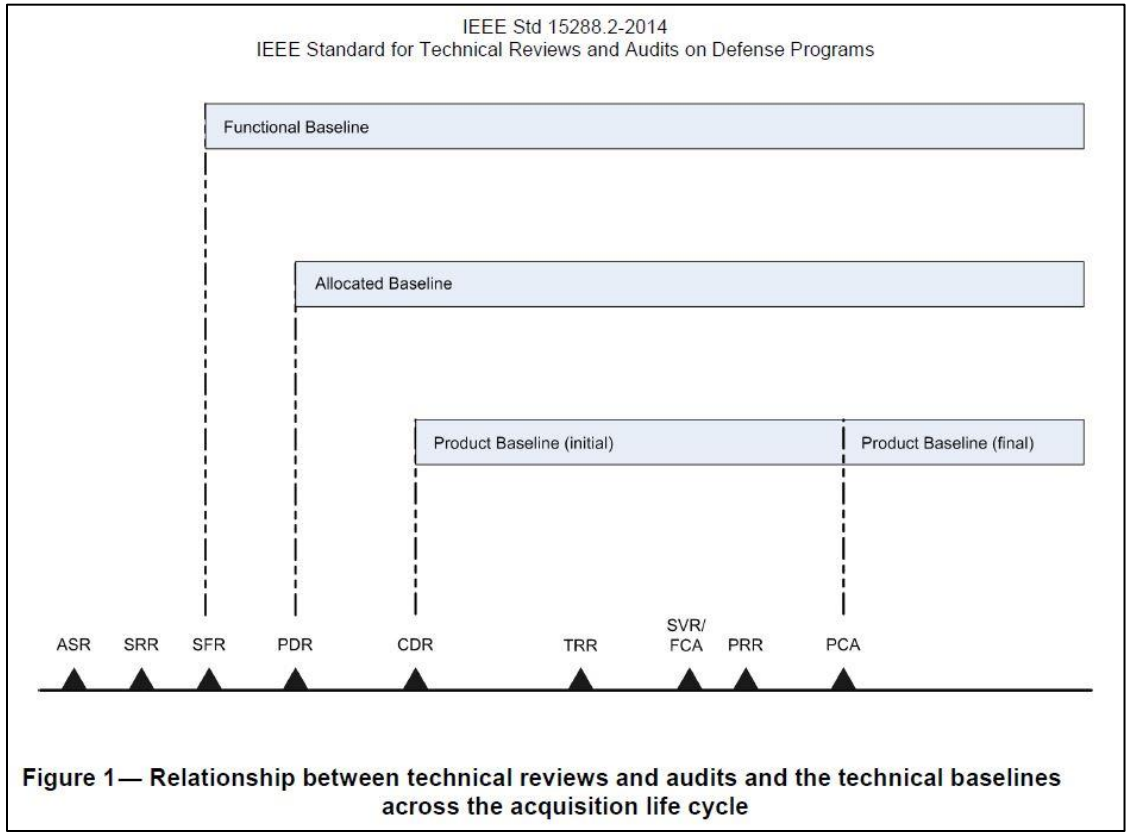
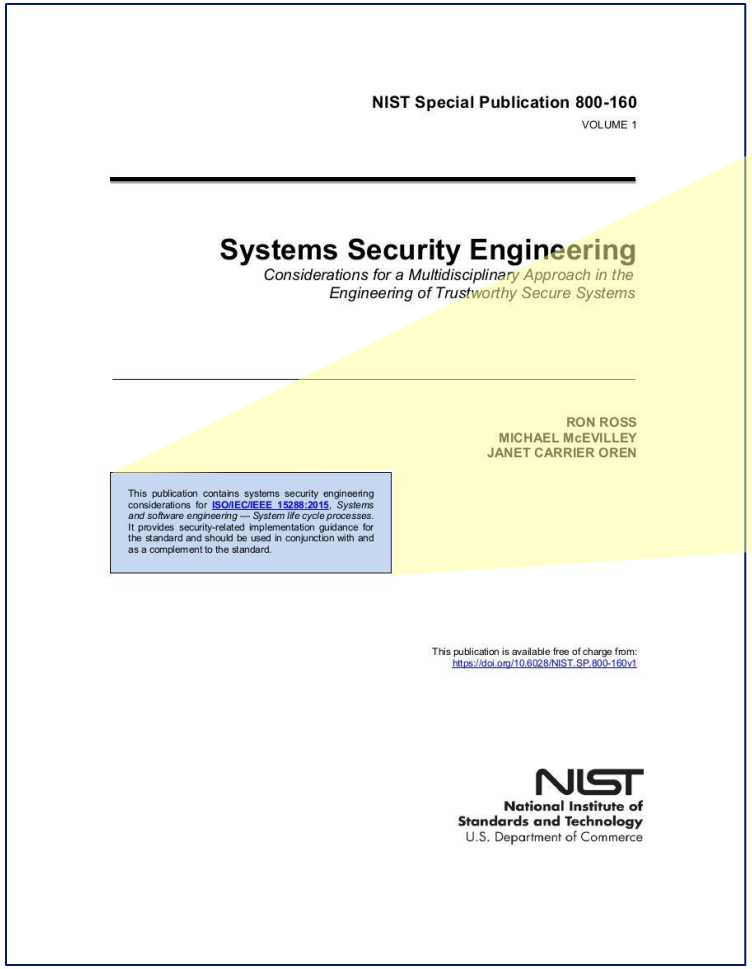


Figure 1— Relationship between technical reviews and audits and the technical baselines across the acquisition life cycle

- The acquirer's SEP, and the supplier's Systems Engineering Management Plan (SEMP) where applicable, should define the technical reviews and audits selected for the program and their specific phasing across the program's life cycle. This standard provides application content for the following technical reviews and audits:
  - Alternative systems review (ASR)
  - System requirements review (SRR)
  - System functional review (SFR)
  - Preliminary design review (PDR)
  - Critical design review (CDR)
  - Test readiness review (TRR) [contained within the program's Test and Evaluation Master Plan (TEMP)]
  - Functional configuration audit (FCA)
  - System verification review (SVR)
  - Production readiness review (PRR)
  - Physical configuration audit (PCA)

NIST SP 800-160v1 IS PER ISO/IEC/IEEE 15288:2015(E)



NIST Special Publication 800-160

VOLUME 1

Systems Security Engineering

Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

RON ROSS
MICHAEL McEVILLEY
JANET CARRIER OREN

This publication contains systems security engineering considerations for ISO/IEC/IEEE 15288:2015, *Systems and software engineering — System life cycle processes.* It provides security-related implementation guidance for the standard and should be used in conjunction with and as a complement to the standard.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-160v1

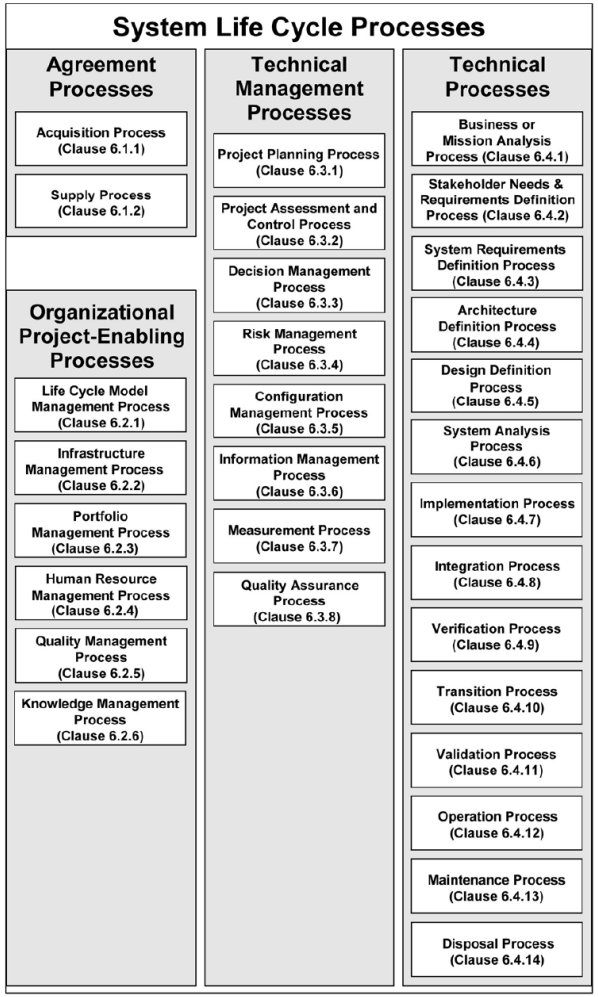
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

This publication contains systems security engineering considerations for ISO/IEC/IEEE 15288:2015, *Systems and software engineering — System life cycle processes.* It provides security-related implementation guidance for the standard and should be used in conjunction with and as a complement to the standard.

NIST SP 800-160v1 is a ISO/IEC/IEEE 15288:2015(E) Security VIEWPOINT

ISO/IEC/IEEE 15288:2015(E), SYSTEMS AND SOFTWARE ENGINEERING – SYSTEM LIFE CYCLE PROCESSES

ISO/IEC/IEEE 15288



NIST SP 800-160 System Life Cycle Processes

3.1 AGREEMENT PROCESSES

- 3.1.1 Acquisition Process
- 3.1.2 Supply Process

3.2 ORGANIZATIONAL PROJECT-ENABLING PROCESSES

- 3.2.1 Life Cycle Model Management Process
- 3.2.2 Infrastructure Management Process
- 3.2.3 Portfolio Management Process
- 3.2.4 Human Resource Management Process
- 3.2.5 Quality Management Process
- 3.2.6 Knowledge Management Process

3.3 TECHNICAL MANAGEMENT PROCESSES

- 3.3.1 Project Planning Process
- 3.3.2 Project Assessment and Control Process
- 3.3.3 Decision Management Process
- 3.3.4 Risk Management Process
- 3.3.5 Configuration Management Process
- 3.3.6 Information Management Process
- 3.3.7 Measurement Process
- 3.3.8 Quality Assurance Process

3.4 TECHNICAL PROCESSES

- 3.4.1 Business or Mission Analysis Process
- 3.4.2 Stakeholder Needs and Requirements Definition Process
- 3.4.3 System Requirements Definition Process
- 3.4.4 Architecture Definition Process
- 3.4.5 Design Definition Process
- 3.4.6 System Analysis Process
- 3.4.7 Implementation Process
- 3.4.8 Integration Process
- 3.4.9 Verification Process
- 3.4.10 Transition Process
- 3.4.11 Validation Process
- 3.4.12 Operation Process
- 3.4.13 Maintenance Process
- 3.4.14 Disposal Process

Change the §6 number in ISO/IEC/IEEE to §3 in NIST SP 800-160 and the section numbering is in alignment

CORELATED ENCLAVE TO PIT SYSTEM / PIT WORK PRODUCTS

Enclave Work Products (Stove-Pipe)

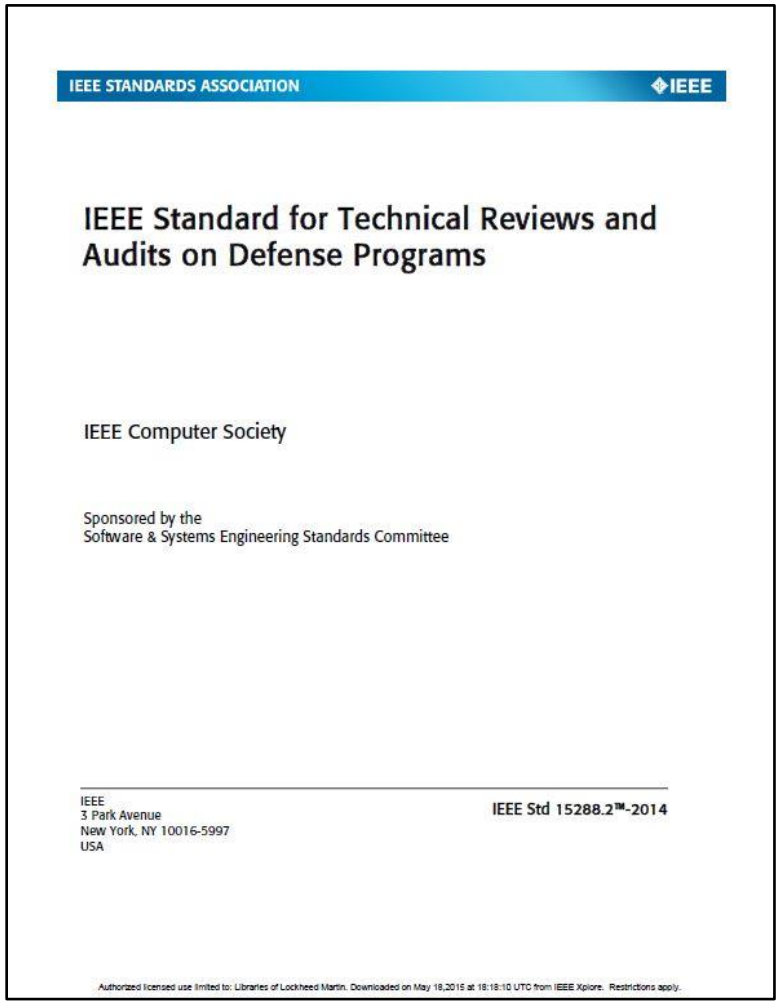
- **Cybersecurity Strategy**
- **System Security Plan (SSP) (RMS KS)**
  - **Ports, Protocols, & Services Management**
  - **DoD Security Control Set**
  - **System Authorization Boundary**
- **Continuous Monitoring Strategy (CMS) (NIST SP 800-137 ISCM)**
- **Security Assessment Plan (SAP)**
- **Security Assessment Report (SAR)**
- **Risk Assessment Report (RAR)**
- **Plan of Action and Milestones (POA&M)**

PIT System / PIT Work Products (Integrated)

- **PPP/PPIP at Appendix E (DoD CIO memo of 20151110 w/template)**
- **System Requirements Specification (SyRS), etc., flow-down Spec.**
  - **§2 Applicable Documents (Internal/External ICDs tied to §6.1 DoDAF SV-1, SV-3)**
  - **§3 Requirements (against HWCI/CSCI Critical Component from PPIP Appendix C) with System-of-Interest C-I-A & Overlays (from NIST SP 800-53r4 and associated CCIs)**
  - **§6.1 Intended Use (to include DoDAF OV-1 High-Level Operational Concept Graphic, DoDAF SV-1 Systems Interface Description, and SV-3 Systems-Systems Matrix)**
- **Cybersecurity Section of SEMP (Tier 1 and/or 2), SyRS §6.1 Intended Use (System-of-Interest Tier 3 Strategy) and PPIP**
- **TEMP Cybersecurity Section & SyRS (w/flow-down) §4 Verification**
- **SyRS (w/flow-down)§4 Verification Reports**
- **Pre MS-A & B Analysis Reports (Design Residual Risk) and Cybersecurity Section of DT&E/OT&E for Requirement Compliance**
  - **Note, the 15288/800-160 (§6.4.2.3e/§3.4.2 SN-5) Analyze Stakeholder Security Requirements Report "Defines" Design SySR Residual Risk for System-of-Interest**
- **Engineering Change Proposal (ECP) / Preplanned Product Improvement (P3I)**

PIT Acquisition Systems Engineering Includes Enclave "Stove-Pipe" Work Products

IEEE STD 15288.2™-2014


IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for Technical Reviews and Audits on Defense Programs

IEEE Computer Society

Sponsored by the
Software & Systems Engineering Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 15288.2™-2014

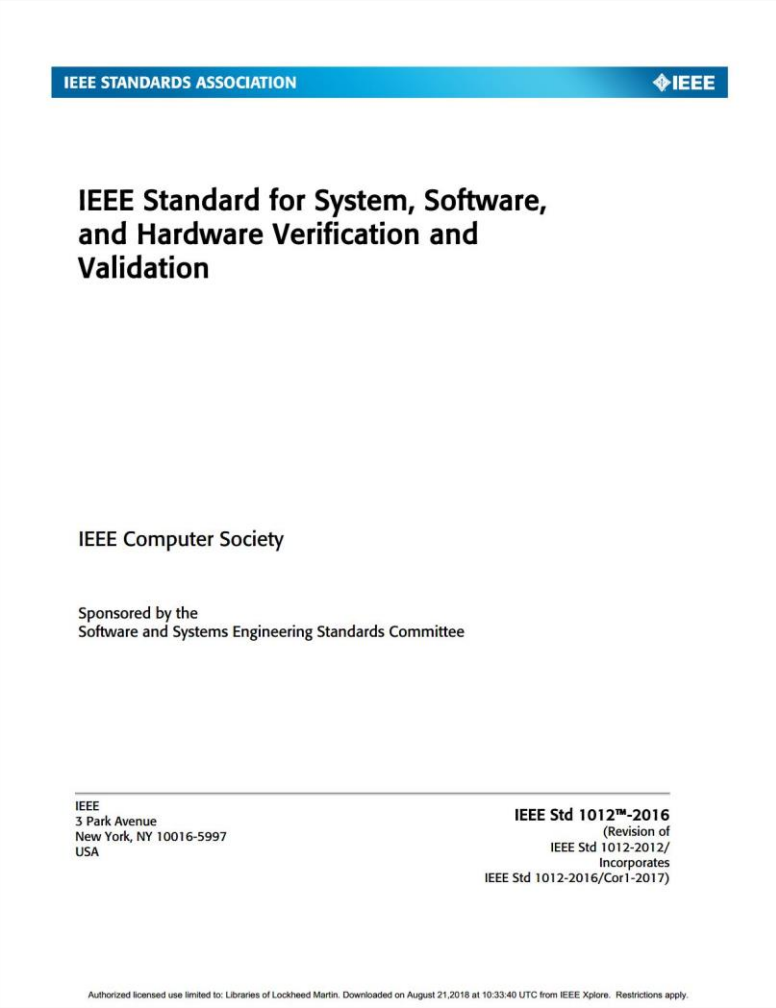
Authorized licensed use limited to: Libraries of Lockheed Martin. Downloaded on May 18,2015 at 18:18:10 UTC from IEEE Xplore. Restrictions apply.

- §6.3 System requirements review (SRR) detailed criteria
- Table 5 – SRR technical review products acceptable criteria
  - **Product: System specification:**

m) System command, control, communication, computer, and intelligence (C4I) requirements are assessed and preliminary performance is allocated across segments and subsystems.
n) System security engineering (SSE), communications security (COMSEC), cybersecurity, and program protection (PP) antitamper security requirements are documented for each preliminary system conceptual architecture in accordance with DoD directives.
o) Preliminary cybersecurity requirements for both hardware and software are documented that address system data protection, availability, integrity, confidentiality, and authentication, and nonrepudiation and are consistent with the National Institute of Standards and Technology (NIST) risk management framework certification and accreditation requirements.
p) Cybersecurity requirements are mapped for each preliminary logical architecture.
q) Threat scenario assessments are completed, threat environments, categories of expected threats and their likelihood of occurrence are defined and correlated with preliminary system logical architectures, survivability and vulnerability KPPs are established for each assessed threat and correlated with the preliminary logical architectures.
hh) Requirements allocations and associated rationale from the source documents to the system specification have been documented.
ii) System specification is approved, including stakeholder concurrence, with sufficiently conservative requirements to allow for design trade space.
Etc.

Cybersecurity is "Built Into" Defense Program Technical Reviews and Audits

IEEE STD 1012™-2016


IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for System, Software, and Hardware Verification and Validation

IEEE Computer Society

Sponsored by the
Software and Systems Engineering Standards Committee

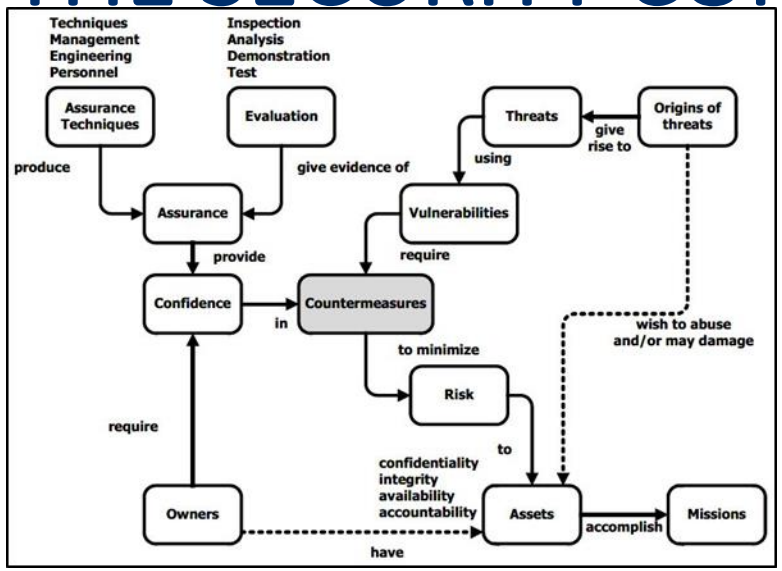
IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 1012™-2016
(Revision of
IEEE Std 1012-2012/
Incorporates
IEEE Std 1012-2016/Cor1-2017)

- Verification and validation (V&V) processes are used to determine whether the development products of a given activity conform to the requirements of that activity and whether the product satisfies its intended use and user needs.
- V&V life cycle process requirements are specified for different integrity levels.
- The scope of V&V processes encompasses systems, software, and hardware, and it includes their interfaces.
- This standard applies to systems, software, and hardware being developed, maintained, or reused (legacy, commercial off-the-shelf [COTS], non-developmental items).
- The term software also includes firmware and microcode, and each of the terms system, software, and hardware includes documentation.
- V&V processes include the analysis, evaluation, review, inspection, assessment, and testing of products.

Cybersecurity is "Built Into" Verification and Validation

IEEE STD 1012™-2016, FIGURE J.1
THE SECURITY CONTEXT OF THE SYSTEM



There are two (2) entrances to "Countermeasures"

- **"Baseline" Assurance to give Owners Confidence in the System-of-Interest**
- **Threats that use Vulnerabilities and Require Countermeasures**

Both are "Mission Driven"

- One of the objectives of security analysis performed by the V&V effort is to verify that the system-required threat controls and safeguards are correctly implemented and to validate that they provide the desired levels of protection of system vulnerabilities. The other objective is to verify that there is a process for describing the system, software, and hardware process security.
- A system should consider different security issues in each phase of the life cycle because the system owner may change as the product evolves. The V&V security analysis should consider:
  - **The context of the system (e.g., the development process and environment, the final operational environment, organization structures and management policy, operational and maintenance personnel roles, interfaces with other external systems or support systems);**
  - **The system of interest and its elements, threats, vulnerabilities, and countermeasures;**
  - **Tradeoffs between techniques, operations, and management to address security requirements.**
  - **Identification of threats. These threats may be natural (e.g., inclement weather, earthquakes), human (e.g., unintended or malicious), or environmental (e.g., chemical leak, power loss).**

Cybersecurity (i.e., Security Context) is "Built Into" Verification and Validation

TADIC-P OR TEST, ANALYSIS, DEMONSTRATION, INSPECTION, CERTIFICATION, AND PROCESS

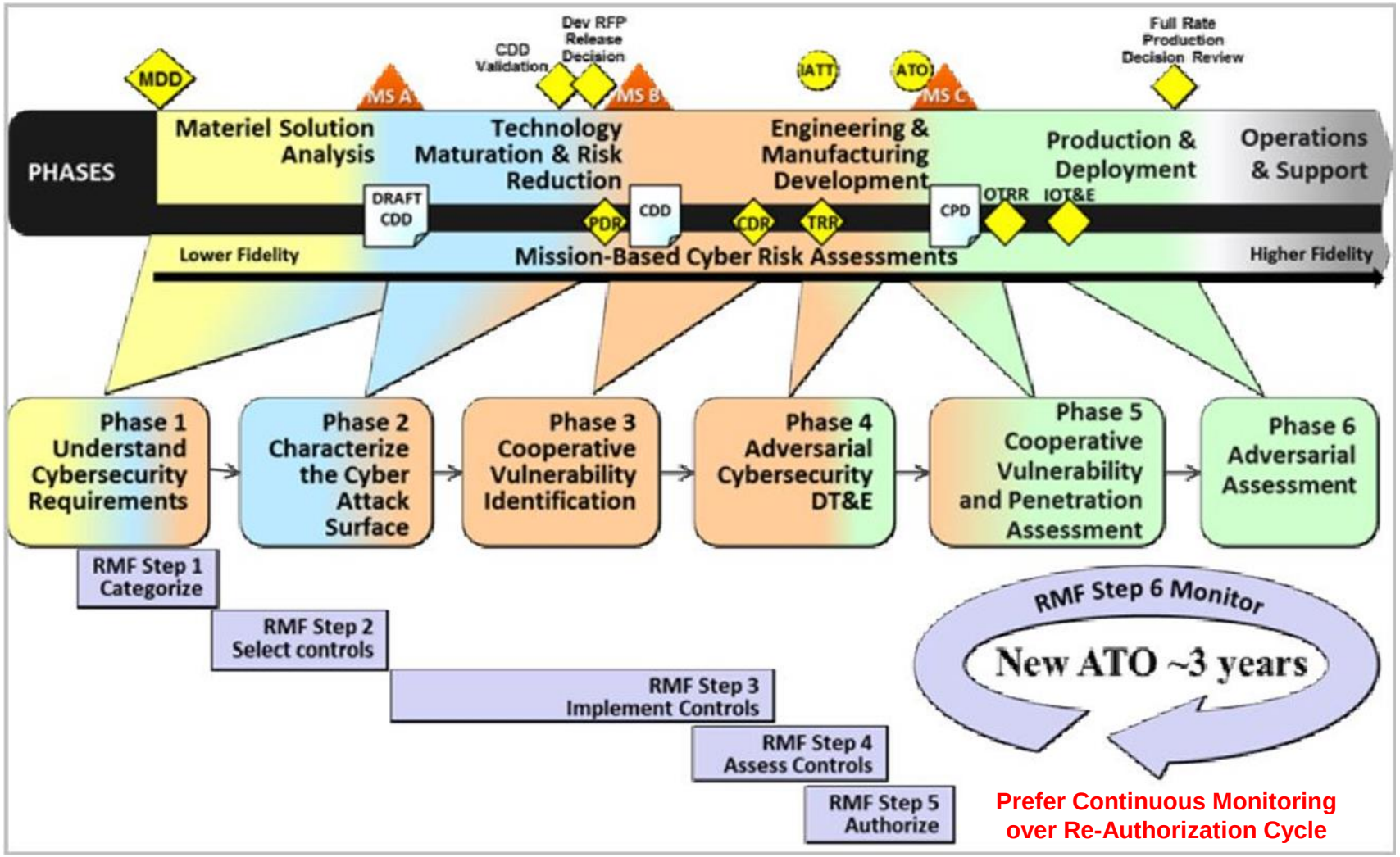
- **Test** – The exercise of hardware, software, and/or operations under specified and controlled conditions using procedures and instrumentation/measuring equipment to verify compliance with quantitatively specified requirements.
- **Analysis or simulation** – Technical evaluation of data using logic, mathematics, modeling, simulation, or analysis techniques under defined conditions to determine compliance with requirements.
- **Demonstration** – The un-instrumented (i.e., special test instrumentation, not the normal delivered system-of-interest self-monitoring instrumentation) exercise of hardware, software, or operations to determine by observation the qualitative performance of specified functions.
- **Inspection** – Examination by the senses (sight, sound, smell, taste, or touch) without the use of special equipment to determine requirements compliance. The NIST SP 800-53Ar4 "Examine" and "Interview" verification methods are special case examples of Inspection.
- **Certification** – When an outside authority (e.g., Underwriter's Laboratory, UL) performs the validation activity to determine requirements compliance and provides a "certification" to that effect.
- **Process** – The case where the evidence of requirement compliance derives from a defined special process because TADIC as defined above cannot verify the requirement. A special process is "a process, the results of which are highly dependent on the control of the process or the skill of the operators, or both, and in which the specified quality cannot be readily determined by inspection or test of the product" (i.e., system-of-interest). (ASME NQA-1-2008/ASME NQA-1a-2009, Part I, §400 Terms and Definitions)

The "How" of a Specification § 4 Verification and Validation is TADIC-P

VERIFICATION AND VALIDATION AND TEST AND EVALUATION SUMMARY

FIGURE 3-4. INTERACTION OF T&E AND RMF CYBERSECURITY ACTIVITIES

- T&E activities are Blue Book-Team / Red Team-Book
  - Integrate Cyber Adversarial Context into the DOT&E TEMP
- RMF activities are Specification TADIC-P driven
  - Always Achieve Specification Compliance or Obtain Deviation / Waver for Non-Compliance

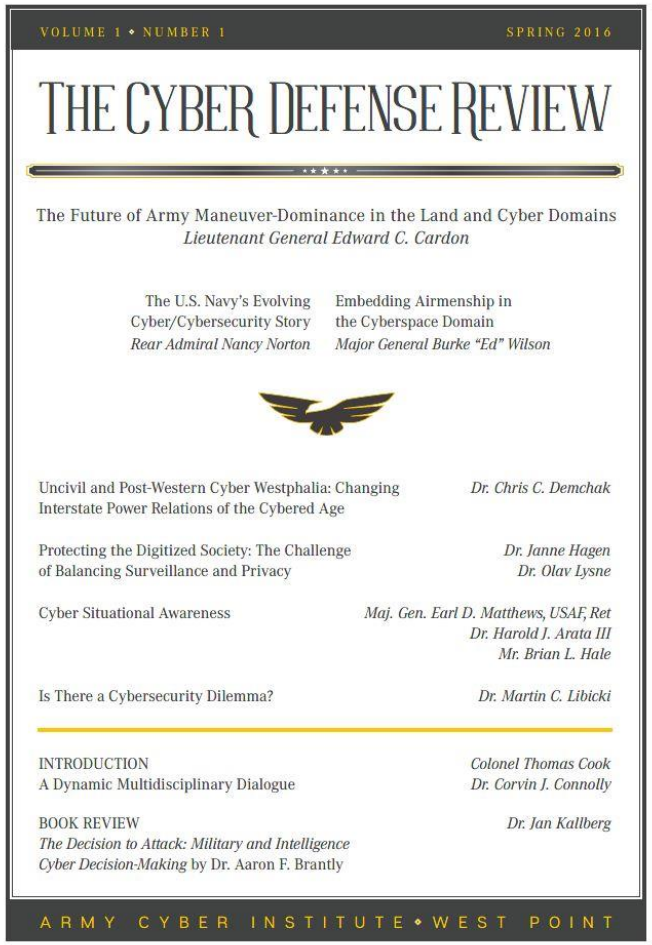


PARALLEL CYBERSECURITY V&V AND T&E

- System Survivability KPP (w/Cyber Survivability – Resiliency)
- Director Operational Test and Evaluation (DOT&E) Test and Evaluation Master Plan (TEMP) “testing” (& Cyber T&E Guidebook v2.0)
  - **Developmental T&E; evidence (Blue Book/Team) you are making progress**
  - **Operational T&E; evidence (Red Team/Book) you have Resiliency**

- Cybersecurity System, Sub-System, and Product Specification §4
- IEEE Std 1012™-2016, IEEE Standard for System And Software Verification and Validation “testing”
  - **Verification; evidence you built the thing right**
  - **Validation; evidence you built the right thing**
  - **Continuous Monitoring for Cyber in Operations and Support (O&S) Phase(?)**

THE BLUE BOOK/TEAM AND RED TEAM/BOOK



VOLUME 1 • NUMBER 1 SPRING 2016

THE CYBER DEFENSE REVIEW

The Future of Army Maneuver-Dominance in the Land and Cyber Domains
Lieutenant General Edward C. Cardon

The U.S. Navy's Evolving Cyber/Cybersecurity Story
Rear Admiral Nancy Norton

Embedding Airmenship in the Cyberspace Domain
Major General Burke "Ed" Wilson

Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age — *Dr. Chris C. Demchak*

Protecting the Digitized Society: The Challenge of Balancing Surveillance and Privacy — *Dr. Janne Hagen, Dr. Olav Lysne*

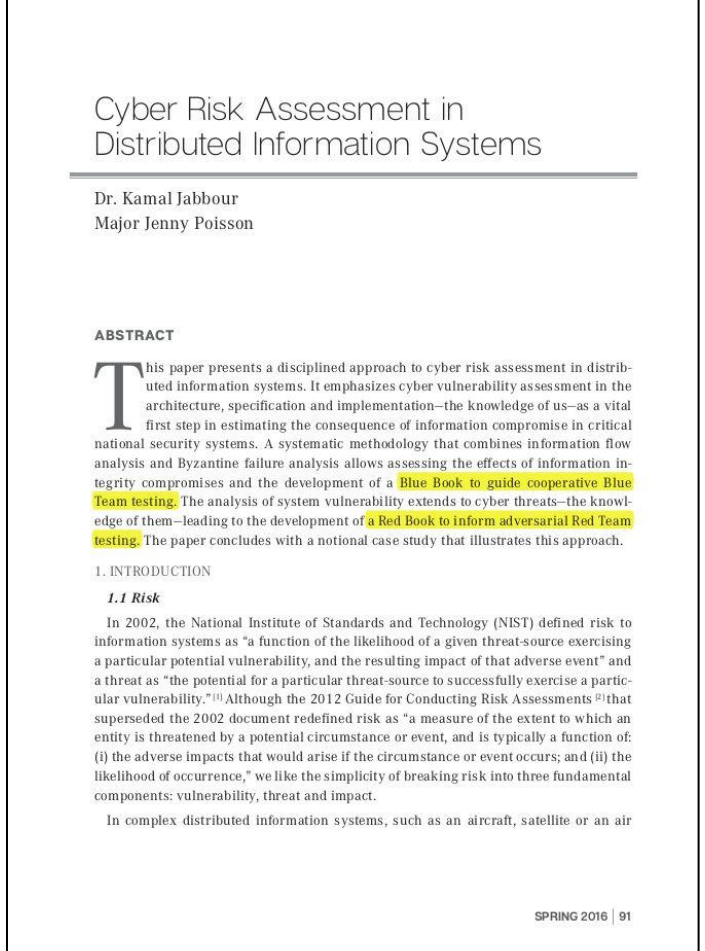
Cyber Situational Awareness — *Maj. Gen. Earl D. Matthews, USAF, Ret, Dr. Harold J. Arata III, Mr. Brian L. Hale*

Is There a Cybersecurity Dilemma? — *Dr. Martin C. Libicki*

INTRODUCTION
A Dynamic Multidisciplinary Dialogue — *Colonel Thomas Cook, Dr. Corvin J. Connolly*

BOOK REVIEW
The Decision to Attack: Military and Intelligence Cyber Decision-Making by Dr. Aaron F. Brantly — *Dr. Jan Kallberg*

ARMY CYBER INSTITUTE • WEST POINT



Cyber Risk Assessment in Distributed Information Systems

Dr. Kamal Jabbour
Major Jenny Poisson

ABSTRACT

This paper presents a disciplined approach to cyber risk assessment in distributed information systems. It emphasizes cyber vulnerability assessment in the architecture, specification and implementation—the knowledge of us—as a vital first step in estimating the consequence of information compromise in critical national security systems. A systematic methodology that combines information flow analysis and Byzantine failure analysis allows assessing the effects of information integrity compromises and the development of a Blue Book to guide cooperative Blue Team testing. The analysis of system vulnerability extends to cyber threats—the knowledge of them—leading to the development of a Red Book to inform adversarial Red Team testing. The paper concludes with a notional case study that illustrates this approach.

1. INTRODUCTION

1.1 Risk

In 2002, the National Institute of Standards and Technology (NIST) defined risk to information systems as "a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event" and a threat as "the potential for a particular threat-source to successfully exercise a particular vulnerability."[1] Although the 2012 Guide for Conducting Risk Assessments [2] that superseded the 2002 document redefined risk as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence," we like the simplicity of breaking risk into three fundamental components: vulnerability, threat and impact.

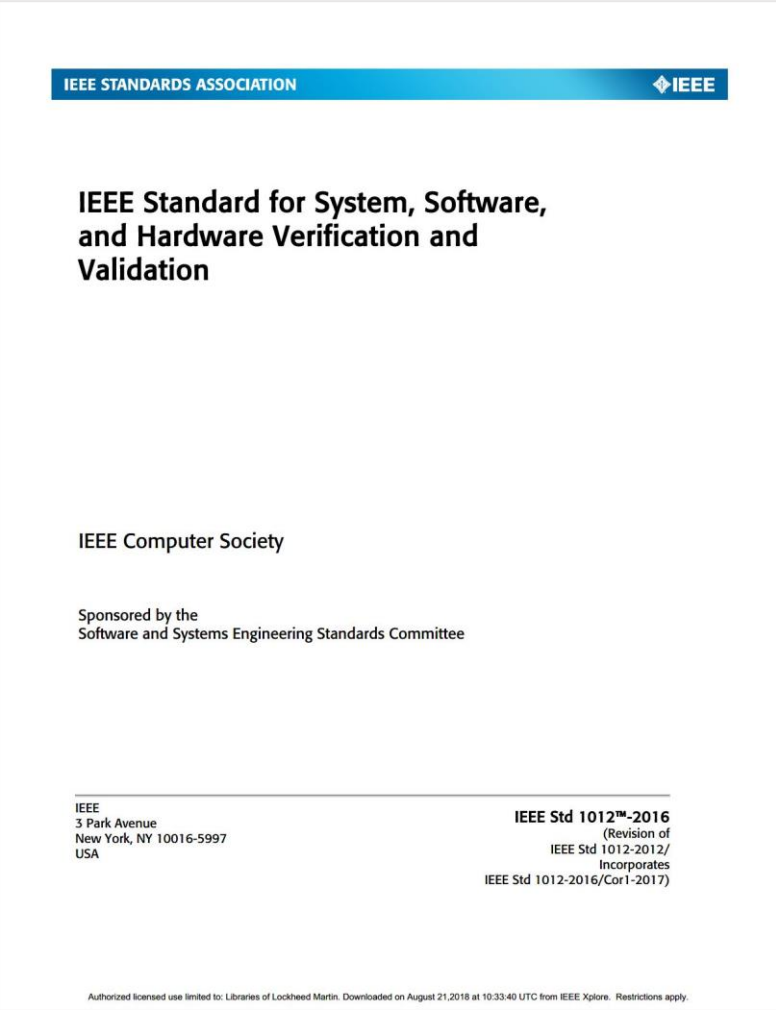
In complex distributed information systems, such as an aircraft, satellite or an air

SPRING 2016 | 91

- The Cyber Risk Assessment (a roadmap)
- Byzantine exploitation
- Separate Vulnerability
  - **Impact or the What**
  - **From Threat or the How**
  - http://www.dtic.mil/docs/citations/ADA635475
  - http://www.dtic.mil/dtic/tr/fulltext/u2/a635475.pdf

Product Life Cycle Centered Mission Based Cyber Risk Assessment (MBCRA)

IEEE STD 1012™-2016



IEEE STANDARDS ASSOCIATION ◆IEEE

IEEE Standard for System, Software, and Hardware Verification and Validation

IEEE Computer Society

Sponsored by the
Software and Systems Engineering Standards Committee

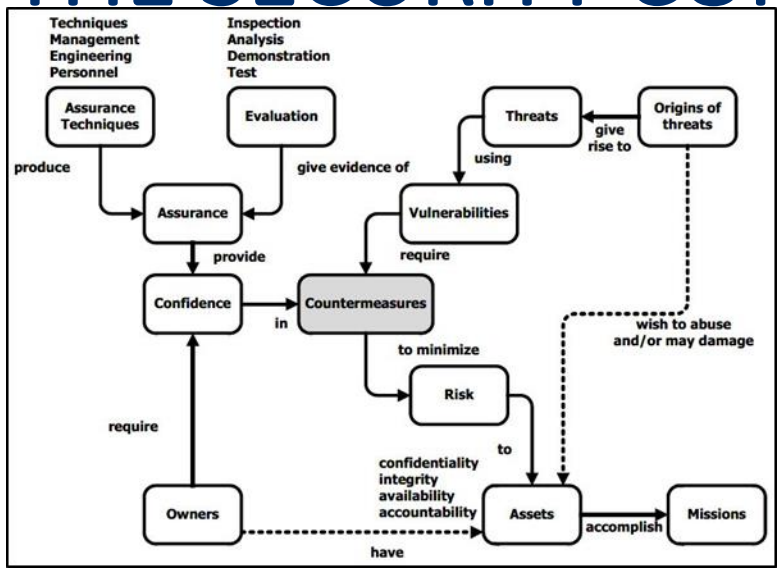
IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 1012™-2016
(Revision of
IEEE Std 1012-2012/
Incorporates
IEEE Std 1012-2016/Cor1-2017)

- Verification and validation (V&V) processes are used to determine whether the development products of a given activity conform to the requirements of that activity and whether the product satisfies its intended use and user needs.
- V&V life cycle process requirements are specified for different integrity levels.
- The scope of V&V processes encompasses systems, software, and hardware, and it includes their interfaces.
- This standard applies to systems, software, and hardware being developed, maintained, or reused (legacy, commercial off-the-shelf [COTS], non-developmental items).
- The term software also includes firmware and microcode, and each of the terms system, software, and hardware includes documentation.
- V&V processes include the analysis, evaluation, review, inspection, assessment, and testing of products.

Cybersecurity is "Built Into" Verification and Validation

IEEE STD 1012™-2016, FIGURE J.1
THE SECURITY CONTEXT OF THE SYSTEM



There are two (2) entrances to "Countermeasures"

- **"Baseline" Assurance to give Owners Confidence in the System-of-Interest**
- **Threats that use Vulnerabilities and Require Countermeasures**

Both are "Mission Driven"

- One of the objectives of security analysis performed by the V&V effort is to verify that the system-required threat controls and safeguards are correctly implemented and to validate that they provide the desired levels of protection of system vulnerabilities. The other objective is to verify that there is a process for describing the system, software, and hardware process security.
- A system should consider different security issues in each phase of the life cycle because the system owner may change as the product evolves. The V&V security analysis should consider:
  - **The context of the system (e.g., the development process and environment, the final operational environment, organization structures and management policy, operational and maintenance personnel roles, interfaces with other external systems or support systems);**
  - **The system of interest and its elements, threats, vulnerabilities, and countermeasures;**
  - **Tradeoffs between techniques, operations, and management to address security requirements.**
  - **Identification of threats. These threats may be natural (e.g., inclement weather, earthquakes), human (e.g., unintended or malicious), or environmental (e.g., chemical leak, power loss).**

Cybersecurity (i.e., Security Context) is "Built Into" Verification and Validation

LOCKHEED MARTIN

SYSTEM SECURITY SYSTEMS ENGINEERING

MFC CYBER SECURITY

SYSTEMS ENGINEERING