A Path Towards Cyber Resilient & Secure Systems Metrics & Measures Framework

October 2015

Holly Dunlap

NDIA SSE Chair
Raytheon
Holly.Dunlap@Raytheon.com

NDIA SSE & DT&E Joint Effort

NDIA SSE Committee Chair
Holly Dunlap

NDIA SSE & INCOSE SSE Committee
Elizabeth Wilson

NDIA DT&E
Joe Manas

Mitre & Chief AF Cyber Integration
Danny Holtzman

Trusted Suppliers Steering Group
Kaye Ortiz

DoD Office of the CIO
Don Davidson

OSD SE PPP
Melinda Reed

Holistic Approach to Program Protection

Frank Kendall directed the streamlining of documents and a holistic approach to system security and program protection on July 18, 2011. Prior to the memo, security was defined and addressed within each security specialty silo leading to inconsistencies and security gaps.

A holistic approach to system security and program protection manages and balances the risks across the security specialties such as anti-tamper (AT), cybersecurity, supply chain, software and hardware assurance, and general program security.

Taking a holistic approach to system security and bringing together multiple communities with rich histories introduces varying perspectives, terminologies, and taxonomies along with methodologies for evaluating the security quality system attributes of metrics and measures.

System Security Challenge

- System Security Challenge
  - Contracts are awarded on technical merit, past performance, and cost.
  - If security relevant requirements are not crisply defined with metrics and measures, system security quality attributes will be traded away to system technical capability and a more affordable solution.
  - Today progress is being made as the presence of security relevant requirements in contract statement of work language is increasing and maturing.
  - However, system security and program protection have not yet made it into the contract award evaluation criteria.

A Case for Change

- **Start with the warfighter in mind**
  - The warfighter has *NEVER* asked for a system that included a specified set of cyber controls.
  - The warfighter has *NEVER* asked for a system that was made in the USA.
  - The warfighter has *NEVER* asked for a system which protects the capability crown jewels for years beyond the current operational mission.

A Case for Change

What the warfighter wants is a system that is:

- ***Resistant*** to kinetic and non-kinetic attack
- ***Resilient*** when under attack

Key Performance Parameters (KPP) are performance attributes of a system considered critical or essential to the development of an effective military capability.

KPPs are expressed in terms of parameters which reflect Measures of Performance (MOPs) using a threshold / objective format.

KPPs must be measurable, testable, and support efficient and effective Test and Evaluation (T&E).

System Survivability

There are (6) mandatory KPP to include the newly defined KPP in the February 12, 2015 release of the JCIDS Manual,

System Survivability (SS)

- **Maintain critical capabilities** under applicable threat environments
- **Reduce the likelihood** of being engaged by hostile fire, through attributes such as speed, maneuverability, detectability, and **countermeasures**;
- **Reduce** the system's **vulnerability** if hit by hostile fire, through attributes such as armor and redundancy of **critical components**;
- Enabling operation in **degraded** EM, space, or **cyber environments**;
- Allow the **system to survive** and continue to operate in, or after exposure to, a CBRN environment, if required.
- In SoS approaches, it may also include **resiliency** attributes pertaining to the ability of the broader architecture to complete the mission despite the loss of individual systems.

Common Metric

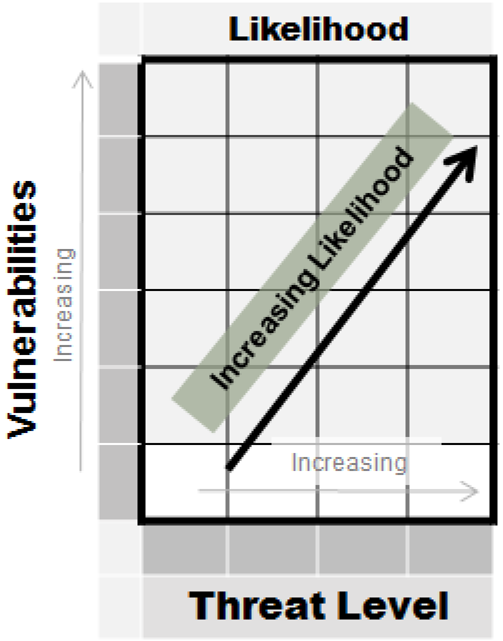
Each security specialty addresses a unique aspect or set of threats and vulnerabilities, and each security specialty has a unique set of countermeasures or risk mitigations.

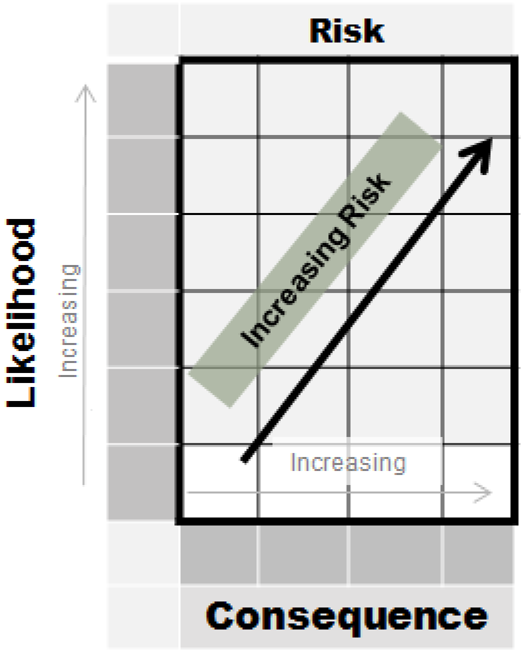
A common metric is needed to communicate across security specialties to minimize the security gaps and seams.

System Security Risk

A common metric across all the security specialties is RISK.

In general terms, risk is calculated as follows:



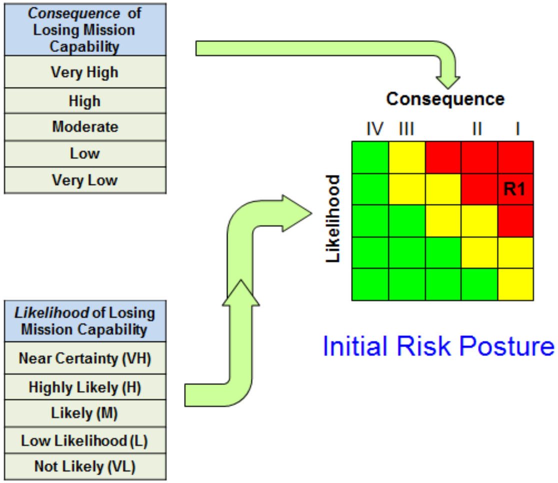


Common Scale for Risk

In order to communicate across security specialties, a common understanding of system security risk is needed.

Each security specialty contributes to system security risk.

Current program protection guidance risk assessment methodology is as follows:



Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

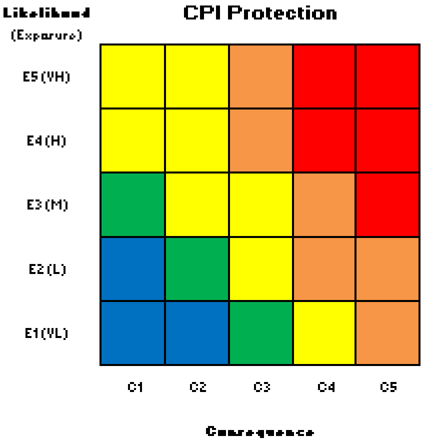
Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Consequence

IV	III		II	I
🟩	🟨	🟥	🟥	🟥
🟩	🟨	🟨	🟥	🟥 R1
🟩	🟩	🟨	🟨	🟥
🟩	🟩	🟩	🟨	🟨
🟩	🟩	🟩	🟩	🟨

Initial Risk Posture

Current CPI risk assessment methodology is as follows:



CPI Protection

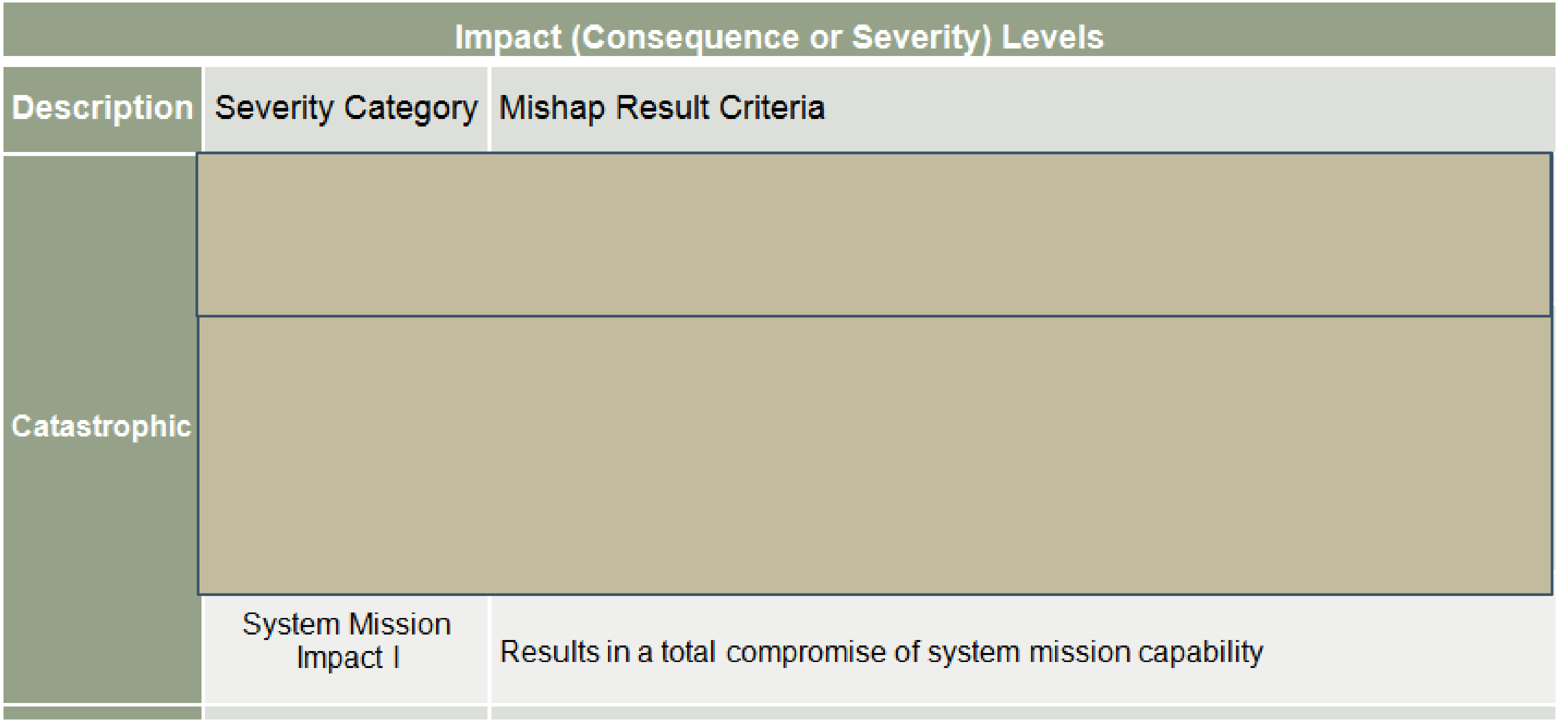
Likelihood (Exposure)					
E5 (VH)	🟨	🟨	🟧	🟥	🟥
E4 (H)	🟨	🟨	🟧	🟥	🟥
E3 (M)	🟩	🟨	🟨	🟧	🟥
E2 (L)	🟦	🟩	🟨	🟧	🟧
E1 (VL)	🟦	🟦	🟩	🟨	🟧
	C1	C2	C3	C4	C5

Consequence

The current example risk ranges vary from 1-3 to 1-5.

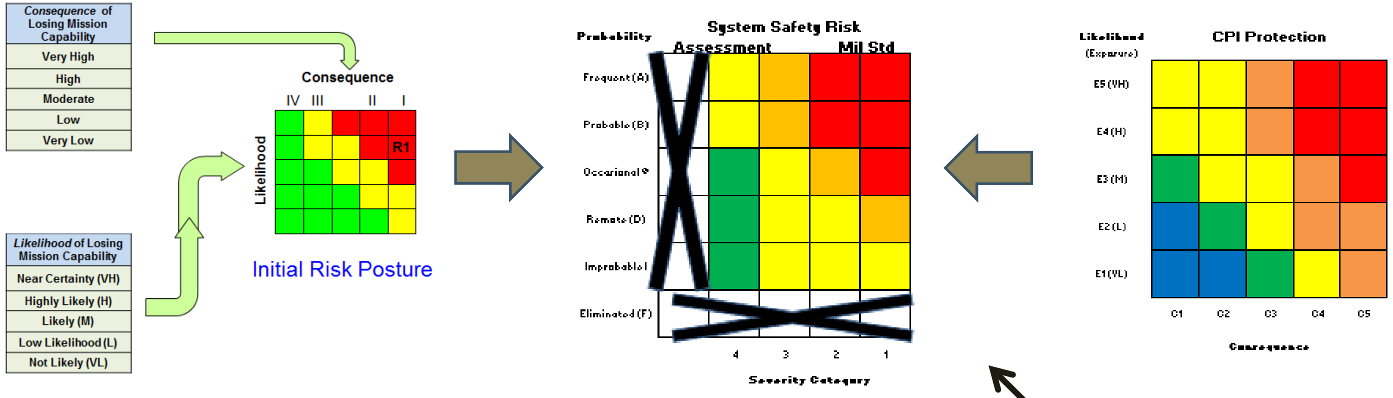
CPI & Safety
Communities with Mature Processes

Bringing together multiple definitions for **Consequence** contributes to developing a richer understanding of consequence and contributes to developing a normalized figure of merit for risk.



Impact (Consequence or Severity) Levels		
Description	Severity Category	Mishap Result Criteria
Catastrophic		
	System Mission Impact I	Results in a total compromise of system mission capability

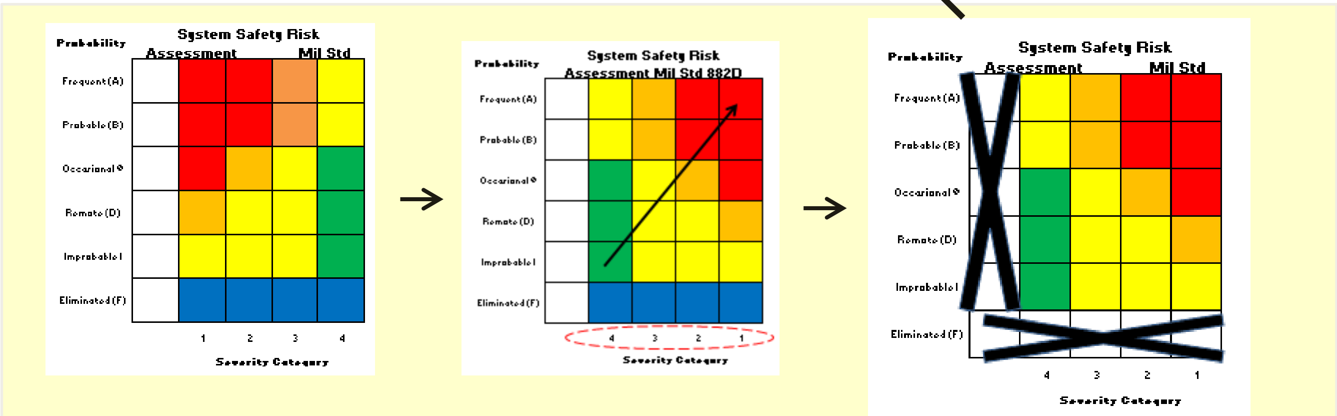
Notional Path To Normalize System Security Risk



Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Initial Risk Posture



Notionally, System Safety Risk Assessment offers a blend between current Program Protection Risk Assessment Methodology and CPI.

Level of Rigor or System Security Risk

- Leverage from Mil-Std 882E, Software Safety Criticality Methodology.
- Resultant equals **either** level of rigor (LOR) required or if the level of rigor specified is not implemented, then the resultant indicates the level of risk that contributes to the overall system safety or in our case system security risk.
- CPI community already use this type of methodology. The resultant of Exposure x Consequence = Level of Protection Required.
- This methodology may also work nicely with supply chain to ensure the authenticity and integrity of components.

Notional Supply Chain LOR / Risk Assessment

Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Consequence

Likelihood	IV	III		II	I
	🟩	🟨	🟥	🟥	🟥
	🟩	🟨	🟨	🟥	🟥 R1
	🟩	🟩	🟨	🟨	🟥
	🟩	🟩	🟩	🟨	🟨
	🟩	🟩	🟩	🟩	🟨

Initial Risk Posture

System Safety Risk Assessment Mil Std

Probability		4	3	2	1
Frequent (A)		🟨	🟧	🟥	🟥
Probable (B)		🟨	🟧	🟥	🟥
Occasional ©		🟩	🟨	🟧	🟥
Remote (D)		🟩	🟨	🟨	🟧
Improbable I		🟩	🟨	🟨	🟨
Eliminated (F)					

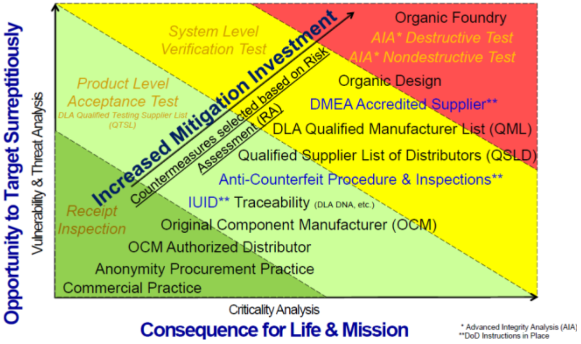
Severity Category

Supply Chain System Security Risk

Likelihood (Escape)	IV	III	II	I
VH	🟨	🟧	🟥	🟥
H	🟨	🟧	🟥	🟥
M	🟩	🟨	🟧	🟥
L	🟩	🟨	🟨	🟧
VL	🟩	🟨	🟨	🟨

Mission Impact

Supply Chain Risk Countermeasures


Opportunity to Target Surreptitiously
Vulnerability & Threat Analysis
Criticality Analysis
Consequence for Life & Mission
Increased Mitigation Investment
Countermeasures selected based on Risk Assessment (RA)
System Level Verification Test
Product Level Acceptance Test
DLA Qualified Testing Supplier List (QTSL)
Receipt Inspection

Organic Foundry

AIA Destructive Test*

AIA Nondestructive Test*

Organic Design

DMEA Accredited Supplier**

DLA Qualified Manufacturer List (QML)

Qualified Supplier List of Distributors (QSLD)

Anti-Counterfeit Procedure & Inspections**

IUID** Traceability (DLA DNA, etc.)

Original Component Manufacturer (OCM)

OCM Authorized Distributor

Anonymity Procurement Practice

Commercial Practice

* Advanced Integrity Analysis (AIA)

**DoD Instructions in Place

Supply Chain Level of Rigor

🟥	Organic Foundry
🟧	System Level Verification Test
🟨	Product Level Acceptance Test
🟩	Receipt Inspection

As microelectronic design complexity and physical feature density increase, the ability to detect counterfeit and malicious modification also increases

Cyber Resilient & Secure System Assurance Case

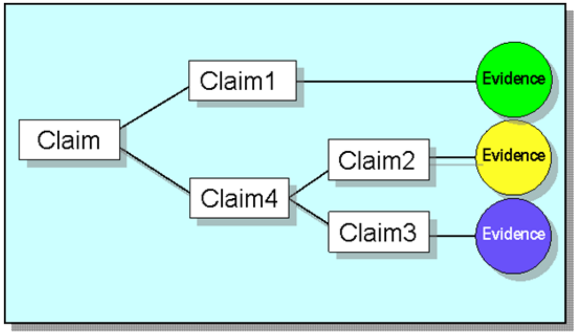


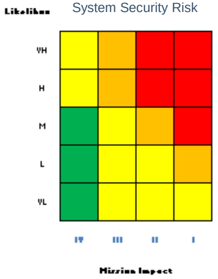
Figure 1: A Structured Argument

Assurance case models provide structured reasoning that engineers use implicitly to gain confidence that systems will work as expected

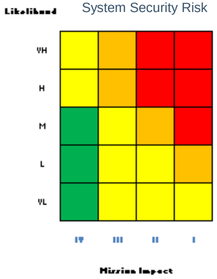
Evidence may include a culmination of tools, techniques, technologies, processes, and expertise.

Evidence of each of the security specialty risk assessments and countermeasures could contribute to an overall system security risk posture

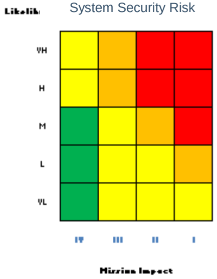
Software Assurance
System Security Risk



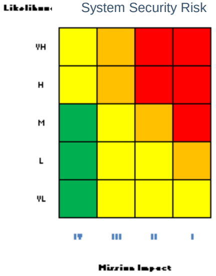
Supply Chain
System Security Risk



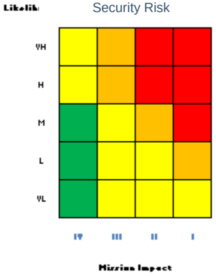
Cybersecurity
System Security Risk



CPI
System Security Risk



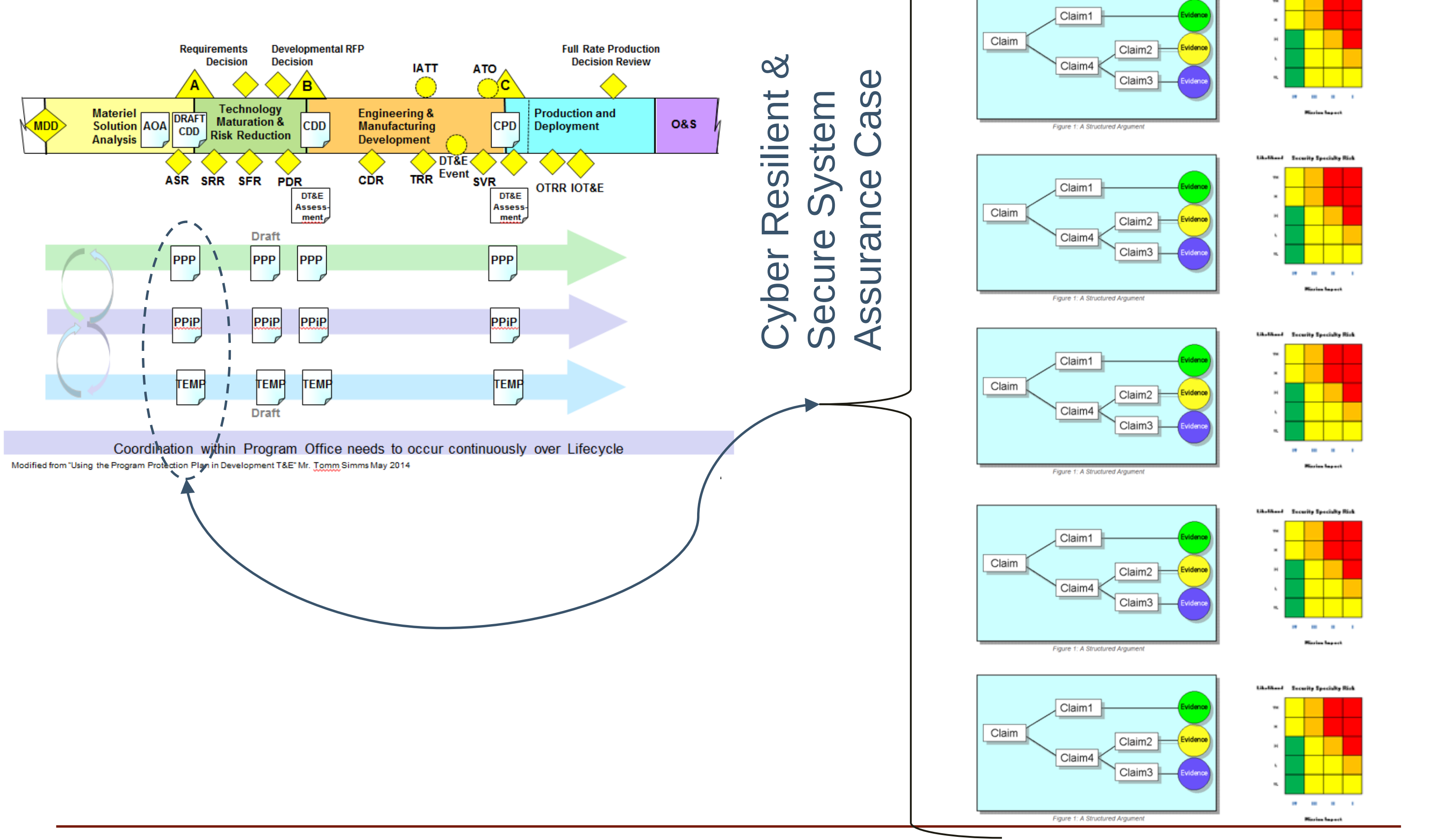
General Program
Security Risk



The layout of each specific security specialty heat maps may differ.
Notionally, the matrix would be the same but the resultant color may differ.

Cyber Resilient & Secure System Assurance Case Matures over the Lifecycle

PPP and TEMP Through Acquisition Lifecycle



Coordination within Program Office needs to occur continuously over Lifecycle

Modified from "Using the Program Protection Plan in Development T&E" Mr. Tomm Simms May 2014

Cyber Resilient & Secure System Assurance Case

Final Thoughts

As defense system integrators and the extended industrial base designs, develops, test, and field systems, it is imperative that we maintain security within the forefront of our priorities. As defense contractors, our actions are powerfully driven by legal contractual requirements. We struggle to conduct system security solution trades that include requirements ambiguity. As individuals, we want to provide the greatest and most advanced trusted capability to the war fighter as quickly as possible.   However, we all work within a cost competitive and customer budget constrained environment. Therefore, crisp well defined requirements matter as does a compelling evidence-based demonstration of why the delivered system can and should be trusted. As defense systems integrators, we want to propose solutions that will be evaluated against known qualitative and quantitative measurable criteria. As business professionals we require work to stay in business and to stay in business we must win contracts. The challenge is technically, politically, financially, and procedurally complex. Providing true holistic program protection requires a fully committed government, industry, and academic partnership.