Application of Criticality Analysis to Risk-Based Engineering Design

Randy Woods
Director, Systems Security Engineering and Anti-Tamper
Office of the Under Secretary of Defense for Research and Engineering

National Defense Industrial Association
Systems & Mission Engineering Conference
December 6-8, 2021

Briefing Overview

- Criticality Analysis Interface with the OUSD(R&E) Mission Engineering Guide
- Mission Critical Functions (MCFs) and Critical Components (CCs)
  - Defined in policy
  - Expanded in guidance
- Criticality Analysis Process
- Example of a Criticality Analysis for a Software Defined Radio (SDR)-based Electronic Warfare System
  - Completion of the Criticality Analysis Table (hardware, software, and custom devices)
  - Selection of protection measures based on type of component
  - Tracking and mitigating risks to critical components (hardware, software, and custom devices)

DoD Mission Engineering Guide
OUSD(R&E) Engineering

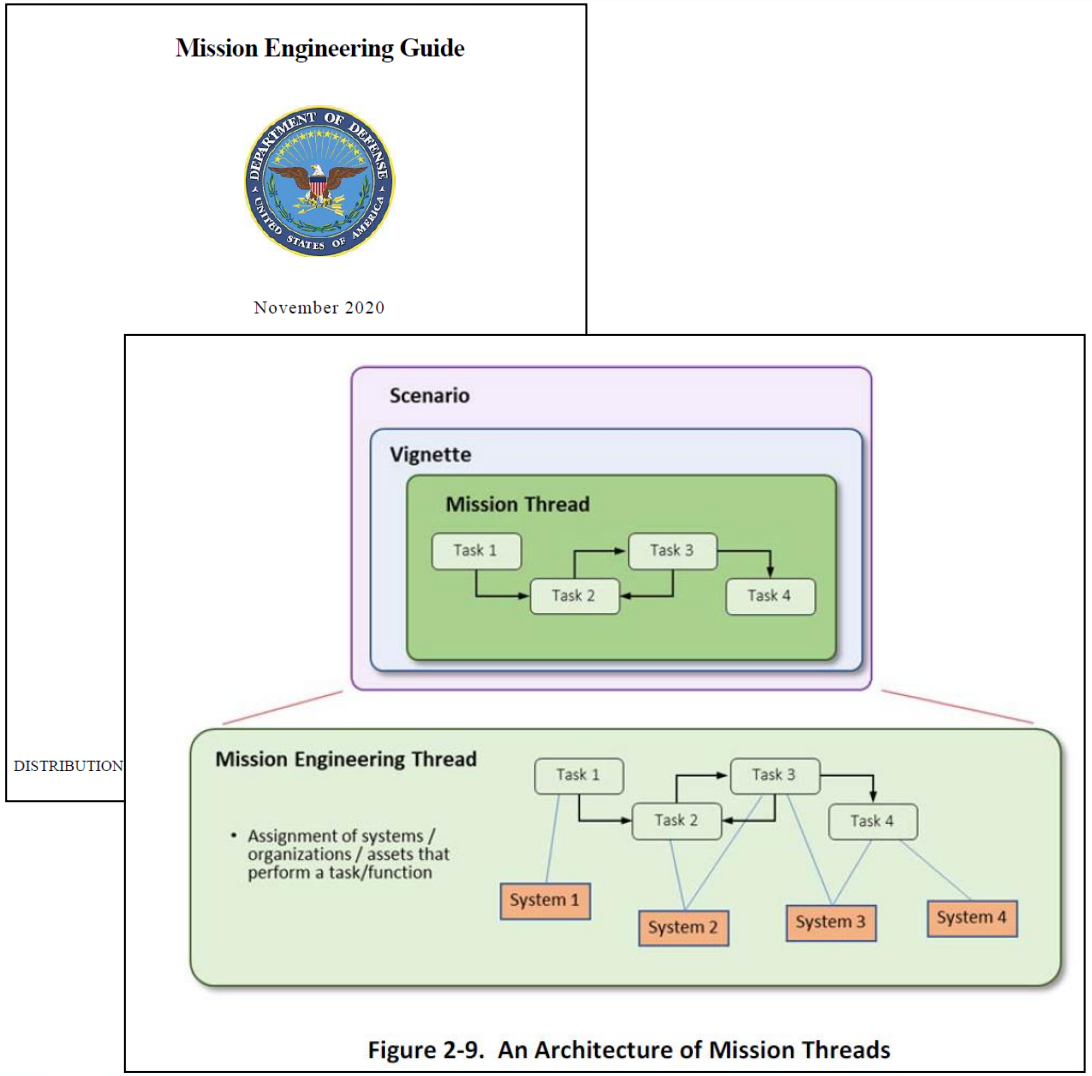
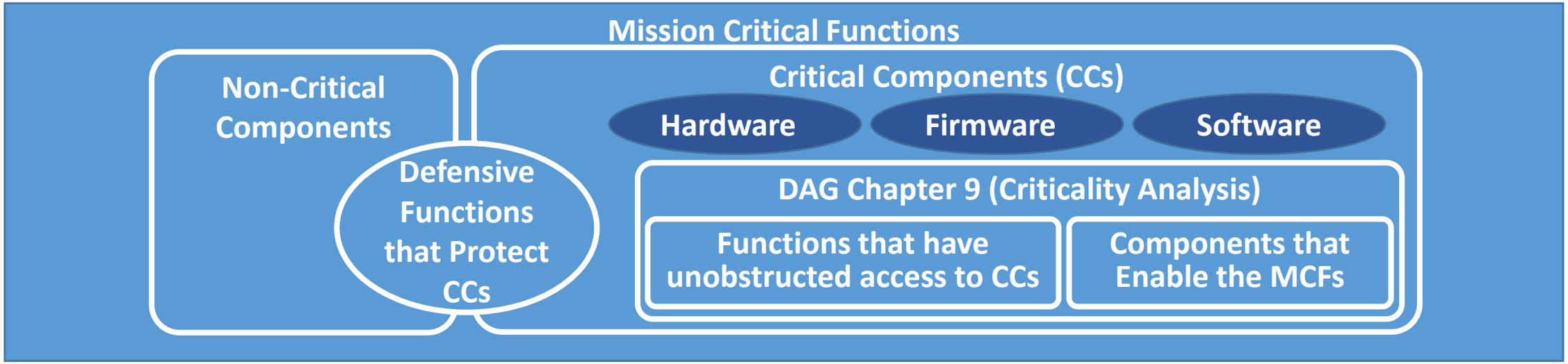


Figure 2-9. An Architecture of Mission Threads

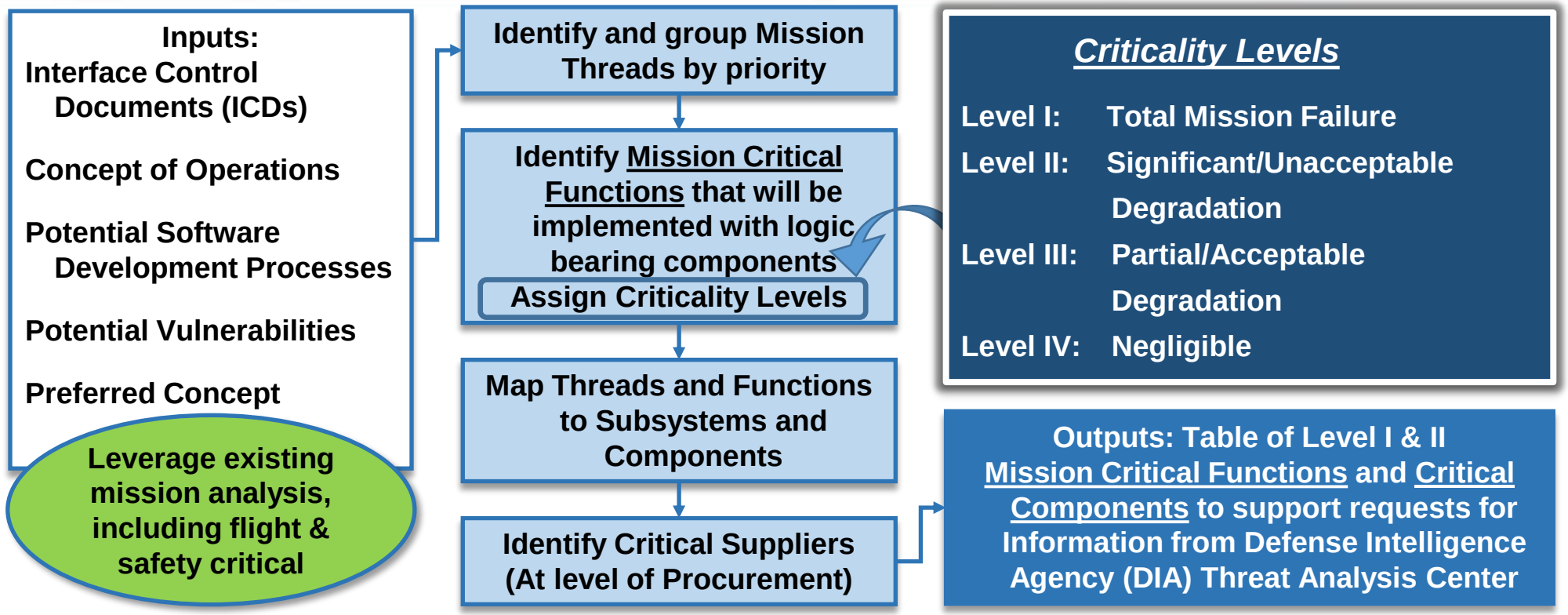
- Describes the foundational elements and the overall methodology of DoD Mission Engineering.
- The Mission Engineering Guide's products include creating Government referenced architectures in the form of diagramed depictions of missions and interactions among elements associated with missions and capabilities.
  - Identify mission threads and principal system functions (tasks).
  - If possible or necessary, group the mission capabilities by relative importance.
    - Training or reporting functions may not be as important as core mission capabilities.
  - Identify the system's MCFs based on mission threads and the likelihood of mission failure if the function is corrupted or disabled.

DoD Instruction 5200.44 and Defense Acquisition Guidebook: Mission Critical Functions and Components



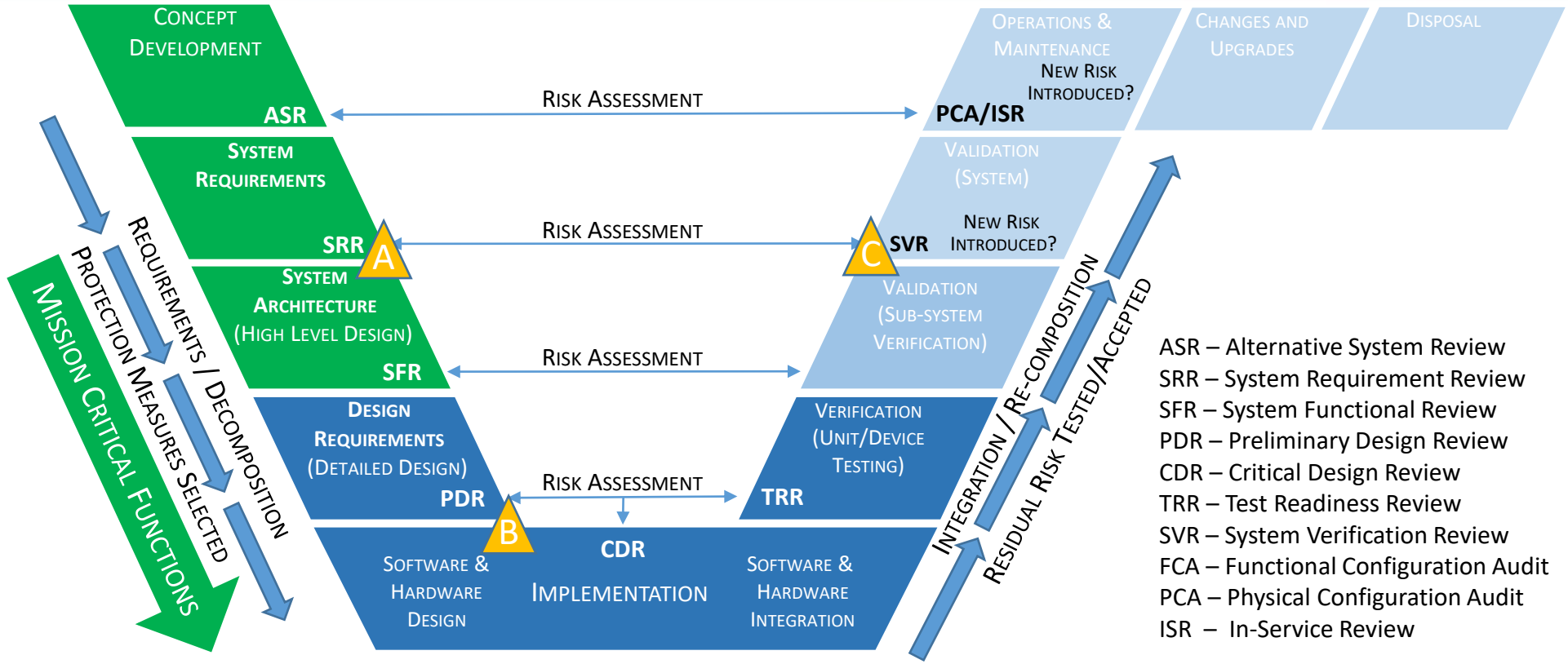
- **Mission Critical Functions (MCFs):**
  - Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed (Source: DoDI 5200.44)
- **Critical Components (CCs):**
  - **A component which is or contains information and communications technology (ICT)** including **hardware, software, and firmware**, whether custom, commercial, or otherwise developed and **delivers or protects** mission critical functionality of a system or which, because of the system's design, **may introduce vulnerability to the mission critical functions** of an applicable system (Source: DoDI 5200.44, 4140.01, and 4140.67)

Criticality Analysis DoD Instruction 5200.44 Definition and Methodology



An end-to-end **functional decomposition** performed by systems engineers to **identify mission critical functions (MCFs) and components**. Includes identification of system missions, decomposition into the functions to perform those missions, and **traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system mission(s).**

Systems Engineering "V" and Trusted Systems and Networks (TSN) Criticality Analysis



ASR – Alternative System Review
SRR – System Requirement Review
SFR – System Functional Review
PDR – Preliminary Design Review
CDR – Critical Design Review
TRR – Test Readiness Review
SVR – System Verification Review
FCA – Functional Configuration Audit
PCA – Physical Configuration Audit
ISR – In-Service Review

	ASR	SRR	SFR	PDR	CDR	SVR/ FCA
Criticality Analysis (CA)	Mission based functions	System requirements	Sub-system/ Sub-function Level	Assembly/ component	Component (updated)	Component (updated)

Trusted Systems and Networks Analysis Matrix – MCFs and CCs

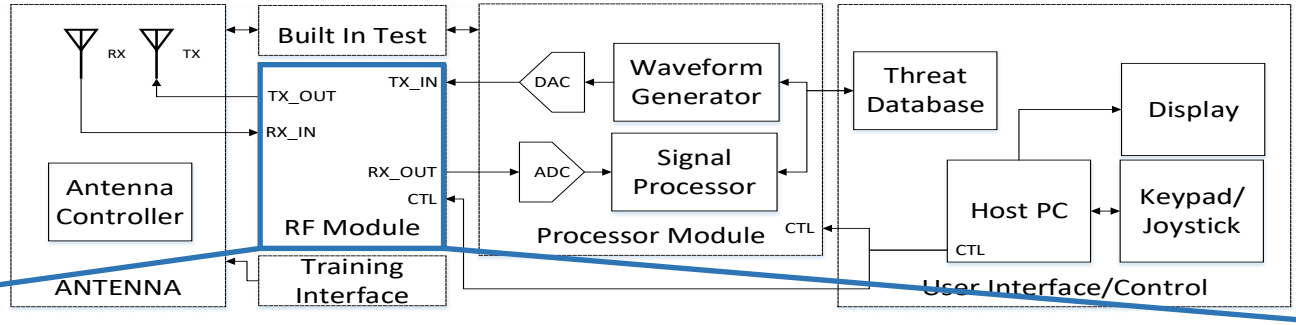
Criticality Analysis (CA)

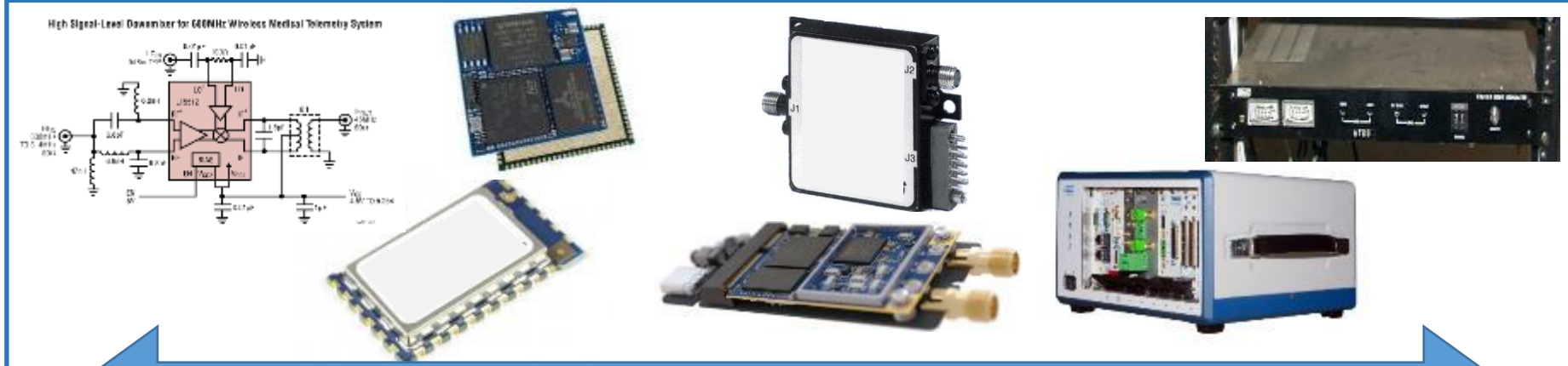
Mission Criticality (System/Functions)

Risk	Level IV	Level III	Level II	Level I
High / Medium / Low	Negligible	Partial/ Acceptable	Significant/ Unacceptable Degradation	Total Mission Failure
Near Certain			DAG Chapter 9 and TSN Guidebook direct Projects and Programs to track level I and II MCFs as part of the PPP. Level I and II Components should be submitted to DIA for SCRM TAC Reports	
Highly Likely				
Likely				
Low Likelihood				
Not Likely				

- The Criticality Analysis is designed to select the **column** for the system.
- Once level I and II systems are identify they are tracked in the PPP as critical components.
- Components with a “low” risk should still be tracked to enable future vulnerabilities to be identified.

Criticality Analysis Example: Block Diagram for SDR-based System

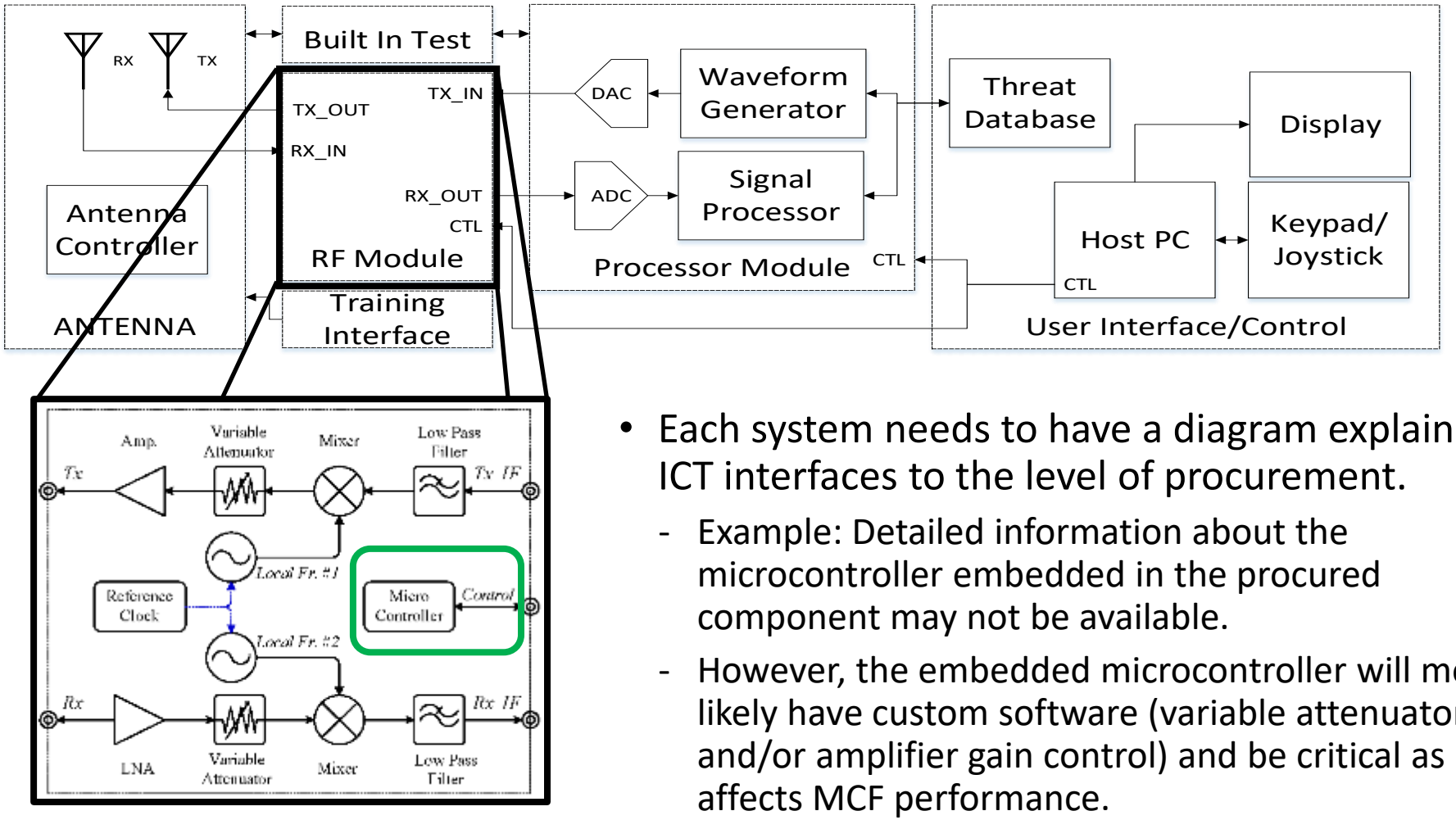




Board Mounted Components (Microcircuits) → **Electronic Assembly (System on Chip and Modules)** → **Electronics Modules**

Critical Components will be procured at different levels from individual microelectronics to rack mounted enclosures depending on program requirements

Criticality Analysis: Level of Procurement

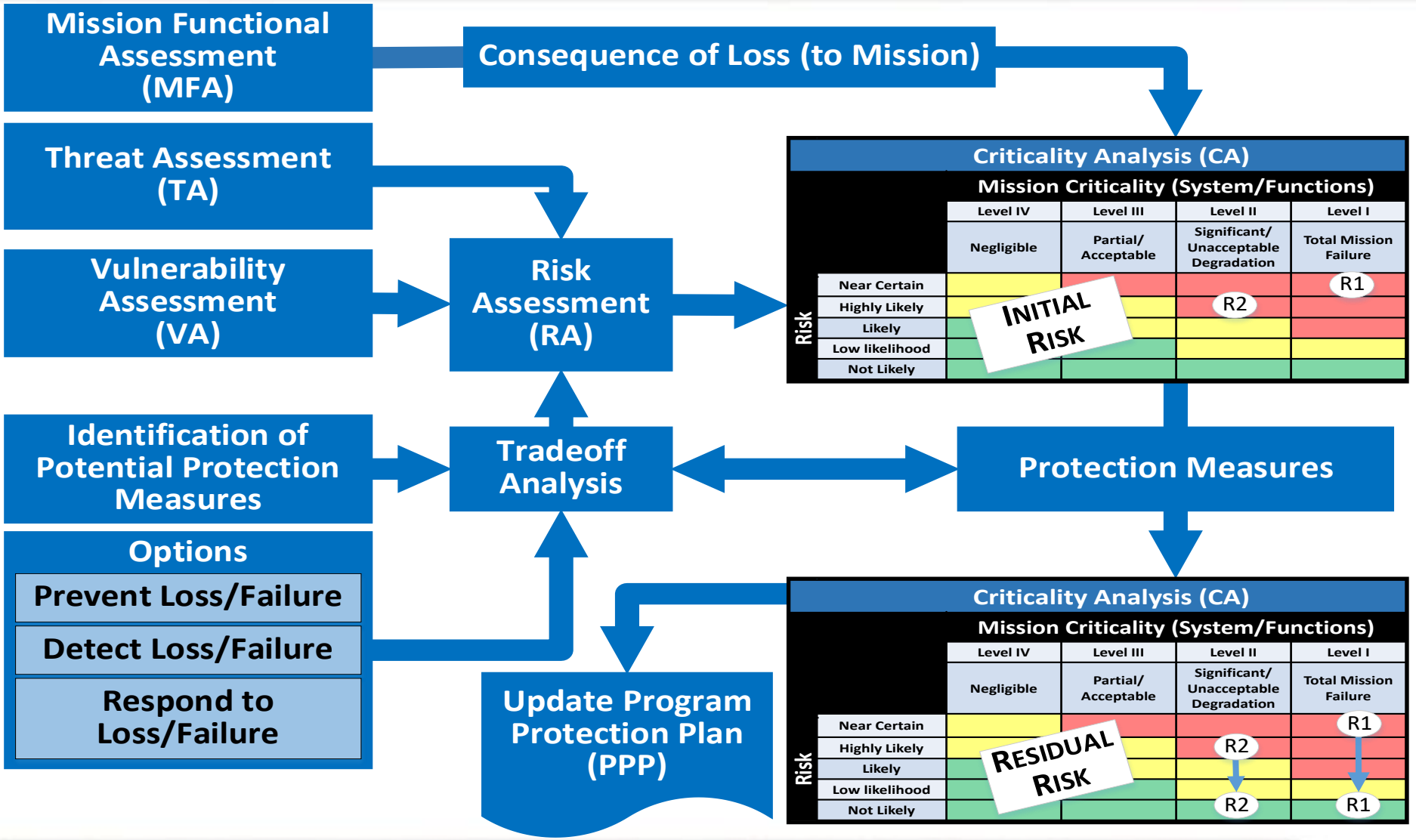


- Each system needs to have a diagram explaining ICT interfaces to the level of procurement.
  - Example: Detailed information about the microcontroller embedded in the procured component may not be available.
  - However, the embedded microcontroller will most likely have custom software (variable attenuator and/or amplifier gain control) and be critical as it affects MCF performance.

Mission Functional Assessment and Criticality Analysis Results

Mission Capabilities	Mission Critical Functions (MCFs)	MCF Criticality Level (I – IV)	Supporting Systems	Critical Components (CCs)	Supplier
Electronic Warfare (Assumed for current example)	Sensing the Environment (Receive)	I	Radar Signal Processor	FPGA 1	Company A
				Signal Processor S/W	Company B
			ADC Unit	ADC Control S/W	Company C
				Comparator 2	Company D
	Analyzing the Environment (Signal Analysis)	II	Receiver Signal Analysis	General Processor 1	Company E
				Signal Database A	Company A
	Responding to the Environment (Technique Generation & High Power Transmission)	I	Waveform Generator	General Processor 2	Company E
				Waveform S/W	Company F
			RF Transmit Module	Power Amplifier	Company G
	Maintenance and Training	III	Built in Test (BIT)	BIT Assembly	Company A
				BIT Control S/W	Company B
			Training Interface	Trainer	Company B

TSN Process



Mission Functional Assessment and Criticality Analysis Results (Software)

Mission Capabilities	Mission Critical Functions (MCFs)	MCF Criticality Level (I – IV)	Supporting Systems	Critical Components (CCs)	Supplier
Electronic Warfare (Assumed for current example)	Sensing the Environment (Receive)	I	Radar Signal Processor	FPGA 1	Company A
				Signal Processor S/W	Company B
			ADC Unit	ADC Control S/W	Company C
				Comparator 2	Company D
	Analyzing the Environment (Signal Analysis)	II	Receiver Signal Analysis	General Processor 1	Company E
				Signal Database A	Company A
	Responding to the Environment (Technique Generation & High Power Transmission)	I	Waveform Generator	General Processor 2	Company E
				Waveform S/W	Company F
			RF Transmit Module	Power Amplifier	Company G
	Maintenance and Training	III	Built in Test (BIT)	BIT Assembly	Company A
				BIT Control S/W	Company B
			Training Interface	Trainer	Company B

- **Document mitigations for each level I and II critical function**
  - Utilize software assurance process (shown) for software items and hardware assurance process for hardware items

Software Protections

Software	Inherent Protection Gained	Supplemental Protection Required	References
Signal Processor	Microkernel with reduced instruction set	Security Tools T1, T2	SDP-CMC
ADC Control	NA	Protection P1 at application layer	SDP-CFF
Signal Database A	NA	Coding std	Best Practices Guide
Waveform	Security tool T3	Coding std P5	www.comapnyF.com/sw/waveformswP5std.pdf

Mission Functional Assessment and Criticality Analysis Results (Custom Microelectronic)

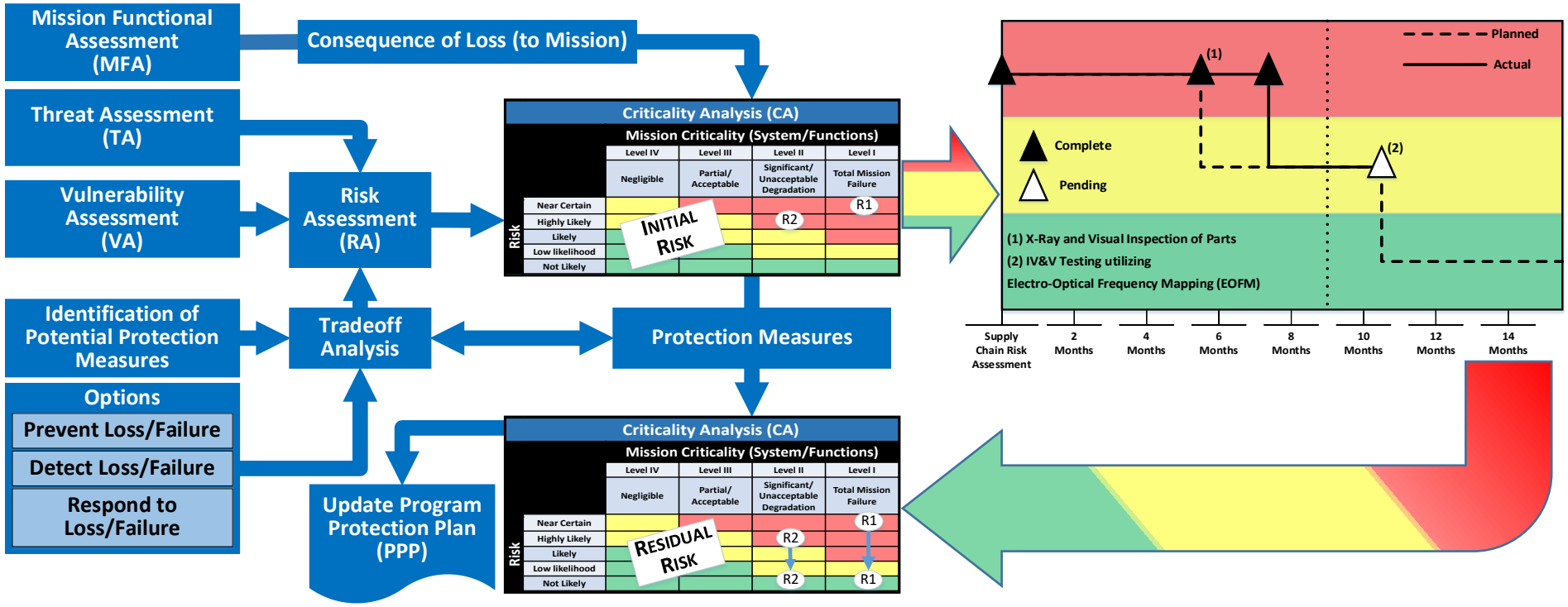
Mission Capabilities	Mission Critical Functions (MCFs)	MCF Criticality Level (I – IV)	Supporting Systems	Critical Components (CCs)	Supplier
Electronic Warfare (Assumed for current example)	Sensing the Environment (Receive)	I	Radar Signal Processor	FPGA 1	Company A
				Signal Processor S/W	Company B
			ADC Unit	ADC Control S/W	Company C
				Comparator 2	Company D
	Analyzing the Environment (Signal Analysis)	II	Receiver Signal Analysis	General Processor 1	Company E
				Signal Database A	Company A
	Responding to the Environment (Technique Generation & High Power Transmission)	I	Waveform Generator	General Processor 2	Company E
				Waveform S/W	Company F
			RF Transmit Module	Power Amplifier	Company G
	Maintenance and Training	III	Built in Test (BIT)	BIT Assembly	Company A
				BIT Control S/W	Company B
			Training Interface	Trainer	Company B

- Customizable components need to be recorded and the intellectual property utilized, with visibility, needs to be tracked.
- Custom Microelectronics approaches are being developed.

Custom Microelectronics Protections

Component	Supplier/Component (CAGE Code)	Intellectual Property (Name and Version)	3rd Party Intellectual Property Visibility
FPGA 1	ACME CAGE CODE: 702SG6	Basic Processor v 3.14	Processor provided by vendor as a hard IP instantiation
	PMA 456	Serial Peripheral Interface (SPI) Bus Controller v 2.1	RTL code provided

Risk Burn Down Exemplar



- Based on the Criticality Analysis, a level of risk can be assigned, utilizing the threat and vulnerability assessments, and tracked during program maturity.
- Risk tracking can be accomplished utilizing a Risk Burn Down Diagram found in the Engineering Risk, Issue, and Opportunity (RIO) Guide.
- As mission criticality increases, the level of acceptable risk should be tracked with the expectation of reaching a lower final risk during system maturation.

Summary

- The Criticality Analysis is expected to evolve along with the program's level of maturity.
  - Should start at the Alternative System Review (ASR) and continue to evolve until the system is designed and integrated.
- The Criticality Analysis is supported by the program performing a vulnerability assessment and obtaining threat assessments for critical components where risk can be assessed.
- The availability of protection measures and risk mitigation is rapidly evolving and is complimentary to the Criticality Analysis Process.
- Components that are identified by the program as "critical components" require special tracking and handling in accordance with the DoD Instruction 4140.01 "Supply Chain Material Management."

Questions