



Field Programmable Gate Array Levels of Assurance and Best Practices Overview

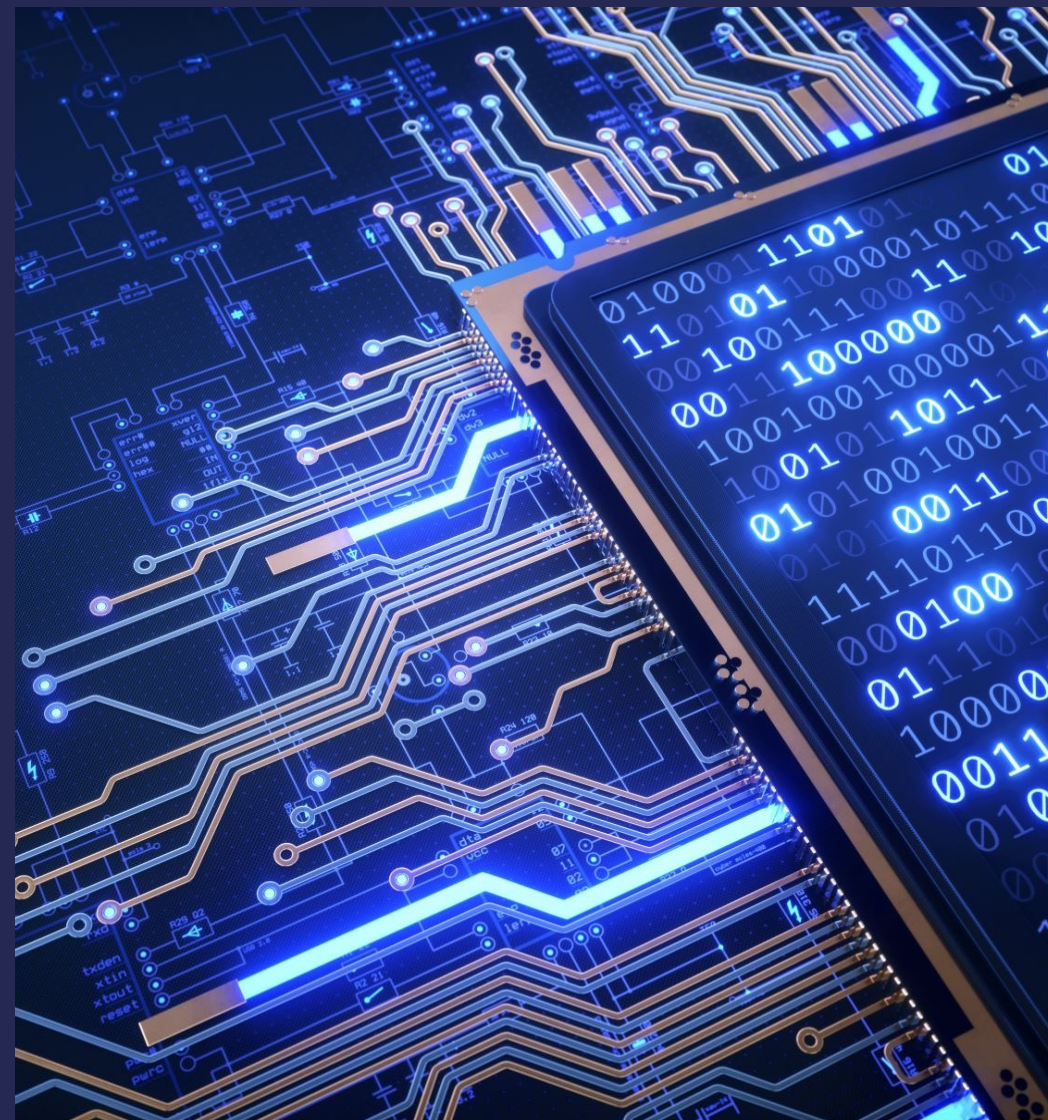
JFAC FPGA Assurance

Jeff Johnson

Technical Director

2023

This entire brief is “Unclassified”





Agenda

Background

Motivation for LoA

LoA Overview

Using the Guidance Overview



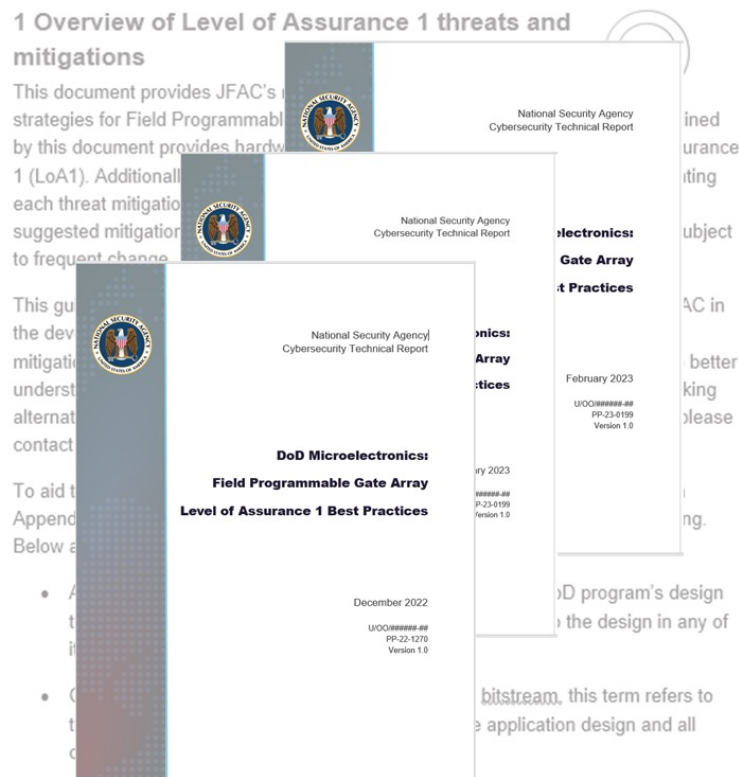
Field Programmable Gate Array (FPGA) LoA Motivation

- The global semiconductor market was ~\$573 billion in 2022 and expected to be ~\$ 1,380.79 billion by 2029.
- Growth is attributed to evolving technologies, such as, artificial intelligence, internet of things, machine learning, consumer electronics, etc.
- FPGA complexity is rapidly expanding to keep up with industry needs.
- The FPGA supply chain is global and presents assurance risk.
- 2019 NDAA mandated the development of hardware assurance standards.
- There was a need for a baseline level of FPGA hardware assurance within DOD.
- NSA, JFAC Technical lead for FPGA assurance, created FPGA Best Practice Guides to ensure programs have FPGA assurance guidance.



Take Action Now

There is enough threat and mitigation information presently available for SMEs to create an initial set of best practices rather than waiting on the outcome of more research.



Output should support existing government policies such as the PPP.

Best practice guidance should be easy to understand and apply. It should lean on existing standards and practices as much as possible.

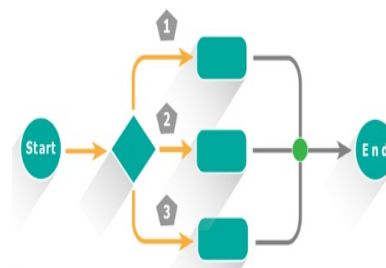
Assurance guidance focus is risk and risk mitigation. Mitigation cost is not a primary driver.



Initial Goals for FPGA Best Practice Guides



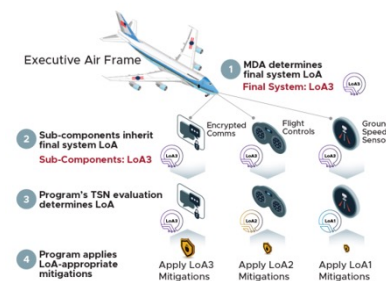
Describe threats and mitigations from the perspective of the USG Program. Mitigations are **performed only by the program**



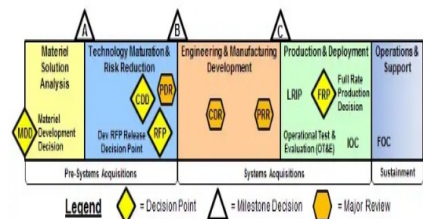
Provide a **consistent framework** with achievable outcomes and **repeatable processes and solutions**



Mitigations are **vendor and product agnostic**



Flows down from the final system to components



Fits within the current DoD acquisition process.

Assurance is the responsibility of USG Programs.



Four Elements of an Assurance Practice

1. LoA Process

- LoA of the top-level system is determined based on criticality
- Further analysis is performed to determine FPGA LOA

Background Document: Field Programmable Gate Array Overall Assurance Process

3. Likelihood Characteristics

“Likelihood” is defined by the

- **Cost** to the adversary to carry out the attack
- **Utility** to the adversary

Background Document: Levels of Assurance Definitions and Applications

2.Threats:

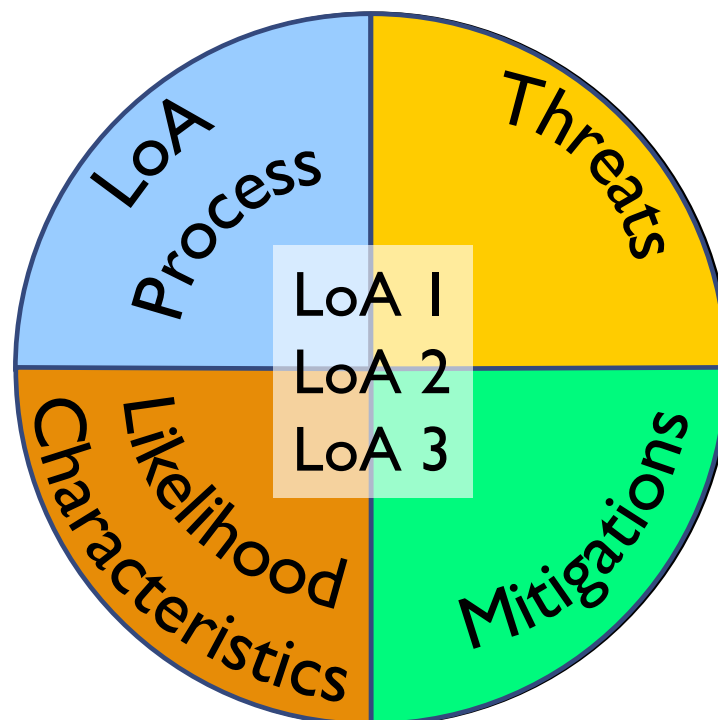
All the attacks with common characteristics or with common mitigations were combined under one of ten threat categories

Background Document: Field Programmable Gate Array Best Practices – Threat Catalog

4. Mitigations

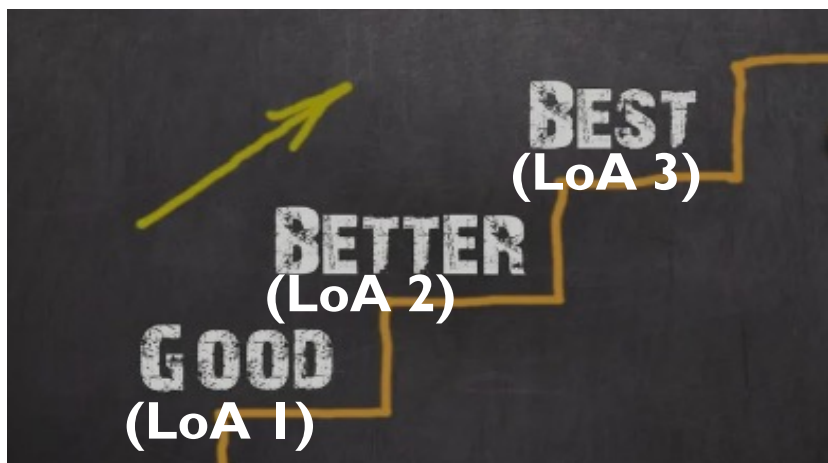
Mitigations for each threat at each LoA were identified

Implementation Documents: Field Programmable Gate Array Level of Assurance 1/2/3 Best Practices and Third-Party IP Review Process for Level of Assurance 1/2/3



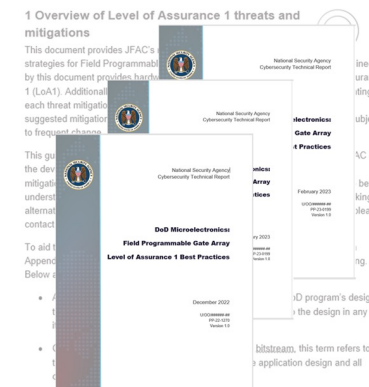
Applicable mitigations by LoA are found in the Best Practices and Third-Party IP Review Process Guides

Three Levels of Assurance



Level of Assurance definition: Provide a level of confidence that a FPGA and its configuration do not contain unexpected characteristics or exhibit unintended behaviors due to the influence of an adversary.

- LoA1 (Acceptable level of confidence)
- LoA2 (Medium level of confidence)
- LoA3 (High level of confidence)



The Program defines the appropriate Level of Assurance

Using the Guidance: Overview

There are four steps to apply LoA guidance:

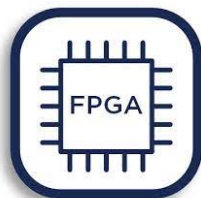
1. Determine System LoA

LoA 1
LoA 2
LoA 3



2. Determine Device LoA

LoA 1
LoA 2
LoA 3



3. Select the appropriate best practice guide.



4. Apply the mitigations






The Program defines the appropriate Level of Assurance



Using the Guidance: Overview

I. Determine the Top-level System LoA



Level of Assurance	Typical Criteria
 LoA1	<p>If the system fails, U.S. Government (USG) capability will be reduced in a meaningful way. If the system is subverted, it can cause harm to U.S. personnel, property, or interests. However:</p> <ul style="list-style-type: none">• Essential operational capabilities for the DoD will remain available even during a system failure.
 LoA2	<p>If the system fails, the consequences will be grave. If the system is subverted, it can cause serious harm to U.S. personnel, property or interest. However:</p> <ul style="list-style-type: none">• Essential operational capabilities for the DoD may be degraded during a system failure and• Redundant capabilities can be brought online as part of the continuity of operations plan, and• The failure of the systems will not cause cascade effects across many DoD or allied systems.
 LoA3	<p>If the system fails, the consequences will be extremely grave. It can cause exceptionally grave harm to U.S. personnel, property or interest. A failure or subversion of this system:</p> <ul style="list-style-type: none">• May represent an existential risk to the USG, and• May cascade across many DoD systems in a way that impacts total operational readiness in an immediate way, and• Will interrupt essential operational capabilities of the DoD.

The LoA of the top-level system determines the highest possible LoA of the subcomponents



Using the Guidance: Overview

2. Determine the Component LoA

- Per the requirement of the Program Protection Plan, each customizable microelectronic device must undergo a Trusted and Secure Network (TSN) evaluation to determine the criticality of the device to the system.
- The TSN criticality result is then mapped to an LoA using the table below.



System LoA	TSN criticality of component to the system			
	Negligible	Partial / Acceptable	Significant / Unacceptable	Total Mission Failure
LoA 1	N/A	LoA 1	LoA 1	LoA 1
LoA 2	LoA 1	LoA 1	LoA 2	LoA 2
LoA 3	LoA 1	LoA 2	LoA 3	LoA 3

2. Determine Device LoA

- LoA 1
- LoA 2
- LoA 3

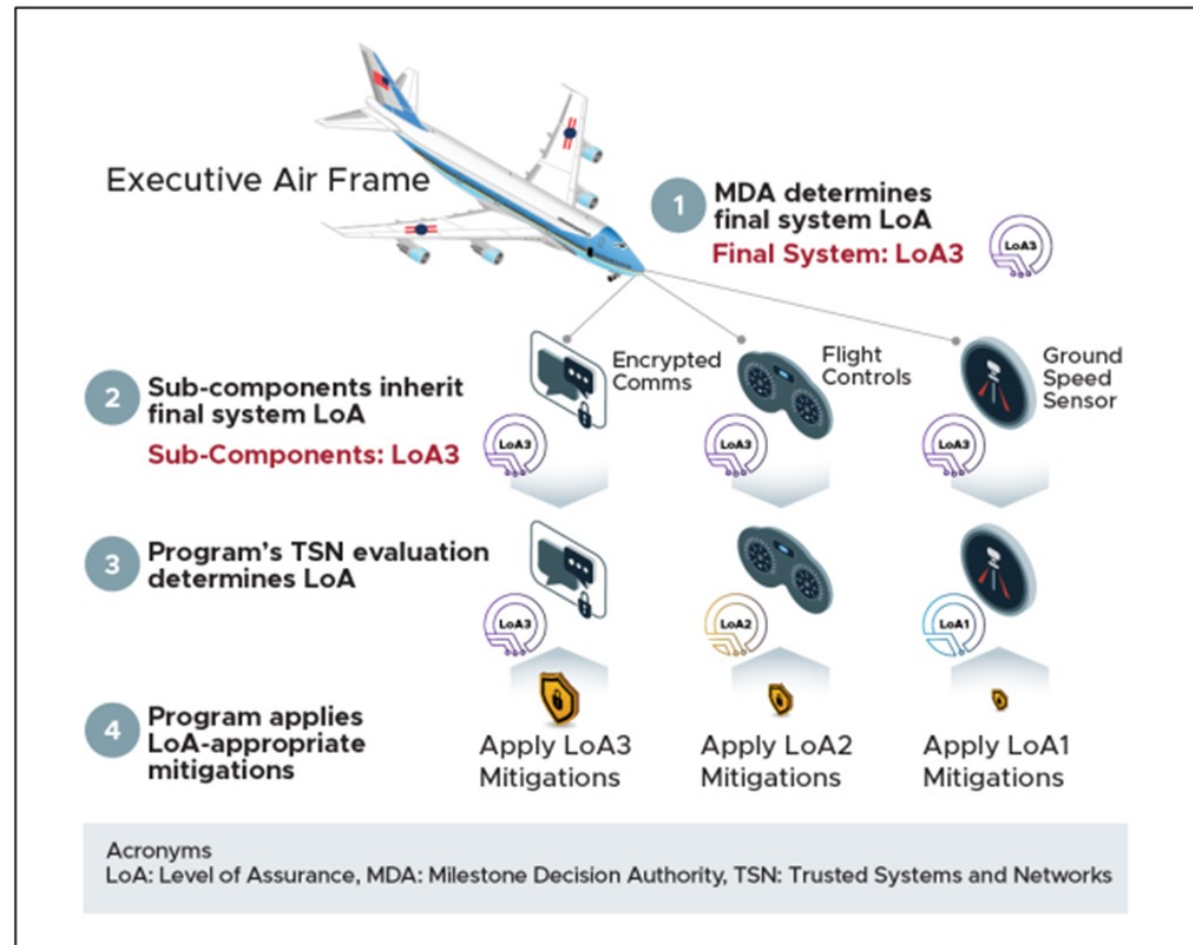


Using the Guidance: Fictional Exemplar

The Process:

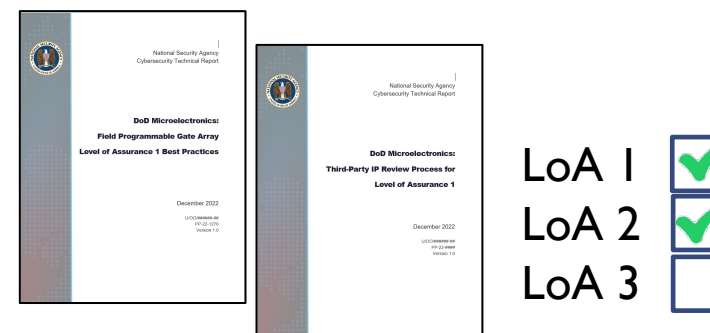
- Determine system LoA
- Subcomponents inherit LoA determination
- Component LoA determined
- LoA Appropriate mitigation applied

System LoA	TSN criticality of component to the system			
	Negligible	Partial / Acceptable	Significant / Unacceptable	Total Mission Failure
LoA 1	N/A	LoA 1	LoA 1	LoA 1
LoA 2	LoA 1	LoA 1	LoA 2	LoA 2
LoA 3	LoA 1	LoA 2	LoA 3	LoA 3





Using the Guidance: Overview



Select the applicable LoA Best Practice Guides

<https://www.nsa.gov/Press-Room/DoD-Microelectronics-Guidance/>



What we need from the community

Ideas, feedback, comments

Please contact us via **JFAC_HWA@radium.ncsc.mil**



THANK YOU

QUESTIONS/COMMENTS: CONTACT
JFAC_HWA@RADIUM.NCSC.MIL